

Exact Random Coding Secrecy Exponents for the Wiretap Channel

Mani Bastani Parizi, *Student Member, IEEE*, Emre Telatar, *Fellow, IEEE*, and Neri Merhav, *Fellow, IEEE*

Abstract—We analyze the exact exponential decay rate of the expected amount of information leaked to the wiretapper in Wyner’s wiretap channel setting using wiretap channel codes constructed from both i.i.d. and constant-composition random codes. Our analysis for those sampled from i.i.d. random coding ensemble shows that the previously-known achievable secrecy exponent using this ensemble is indeed the exact exponent for an average code in the ensemble. Furthermore, our analysis on wiretap channel codes constructed from the ensemble of constant-composition random codes leads to an exponent which, in addition to being the exact exponent for an average code, is larger than the achievable secrecy exponent that has been established so far in the literature for this ensemble (which in turn was known to be smaller than that achievable by wiretap channel codes sampled from i.i.d. random coding ensemble). We show examples where the exact secrecy exponent for the wiretap channel codes constructed from random constant-composition codes is larger than that of those constructed from i.i.d. random codes and examples where the exact secrecy exponent for the wiretap channel codes constructed from i.i.d. random codes is larger than that of those constructed from constant-composition random codes. We, hence, conclude that, unlike the error correction problem, there is no general ordering between the two random coding ensembles in terms of their secrecy exponent.

Index Terms—Wiretap channel, Channel resolvability, Secrecy exponent, Resolvability exponent

I. INTRODUCTION

THE problem of communication in presence of an eavesdropper wiretapping the signals sent to the legitimate receiver (see Figure 1) was first studied by Wyner [1] and later, in a broader context, by Csiszár and Körner [2], where it was shown (among other results) that as long as the eavesdropper’s channel is weaker than legitimate receiver’s channel, reliable and *secure* communication at positive rates is feasible. More precisely, it was shown that, given any distribution on the common input alphabet of the channels, P_X , for which the mutual information developed across the legitimate receiver’s channel is higher than that developed across the wiretapper’s channel, that is, $I(X; Y) > I(X; Z)$, with $(X, Y, Z) \sim P_X(x)W_M(y|x)W_E(z|x)$ (where $X, Y,$

and Z represent the common input, legitimate receiver’s channel output, and wiretapper’s channel output, respectively), as long as the secret message rate $R_s \triangleq \frac{1}{n} \log |\mathcal{S}_n|$ is below $I(X; Y) - I(X; Z)$ there exists a sequence of coding schemes (indexed by the block-length n) using which

$$\lim_{n \rightarrow \infty} \max_{s \in \mathcal{S}_n} \Pr\{\hat{s}_{\text{ML}}(Y^n) \neq S | S = s\} = 0, \quad (1a)$$

$$\lim_{n \rightarrow \infty} \frac{1}{n} I(S; Z^n) = 0. \quad (1b)$$

In the above, S represents the secret message taking values in the message set \mathcal{S}_n , $\hat{s}_{\text{ML}}(Y^n)$ is the maximum-likelihood (ML) estimation of the sent message given the output sequence of the legitimate receiver’s channel and Z^n represents the output sequence of the wiretapper’s channel (see Figure 1).

Classical codes for the wiretap channel are constructed by associating each message with a code that operates at a rate R just below the mutual information developed across the eavesdropper’s channel. To communicate a message, the stochastic encoder of Alice picks a codeword uniformly at random from the code associated to that message and transmits it via consecutive uses of the channel [1]–[3]. Such constructions, known as *capacity-based constructions* (with a slight abuse of terminology) [4], will guarantee that the normalized amount of information that Eve learns about the secret message by observing her channel output signal, $\frac{1}{n} I(S; Z^n)$, will be arbitrarily small, provided that the block-length n is sufficiently large. Recently, *resolvability-based* constructions for wiretap channel codes, namely, those associating each message with a code operating at a rate just above the mutual information of the wiretapper’s channel was shown to be more powerful than the capacity-based constructions to prove achievability results. Indeed, in [5] it was shown that such constructions can be used to easily show that the *unnormalized* amount of information Eve learns about the secret message, $I(S; Z^n)$, vanishes as the block-length increases, namely to establish *strong secrecy* (a notion first introduced by Maurer and Wolf [6]). In particular, when resolvability-based wiretap channel codes are employed over stationary memoryless wiretap channels the amount of information Eve learns about the secret message vanishes *exponentially fast* in the block-length. Thus, it is natural to study the rate of this exponential decay.

Definition 1. Given the rate pair (R_s, R) and a pair of stationary memoryless channels (W_M, W_E) , a number η is an achievable *secrecy exponent* if there exists a sequence of coding schemes of block-length n and secret message rate R_s , each message associated with a sub-code of rate R (i.e., the encoder needs access to a random number generator of rate R)

The authors would like to thank anonymous reviewers for their helpful comments that improved the quality of the manuscript.

The work of M. Bastani Parizi and E. Telatar was supported by the Swiss National Science Foundation (SNSF) grant no. 200020_146832. The work of N. Merhav was supported by the Israel Science Foundation (ISF), grant no. 412/12.

The material in this paper was presented in part in 2016 IEEE International Symposium on Information Theory (ISIT 2016).

M. Bastani Parizi and E. Telatar are with the Information Theory Laboratory (LTHI), Swiss Federal Institute of Technology (EPFL), Lausanne 1015, Switzerland (email: mani.bastaniparizi@epfl.ch, emre.telatar@epfl.ch)

N. Merhav is with the Department of Electrical Engineering, Technion - Israel Institute of Technology, Haifa 32000, Israel (email: merhav@ee.technion.ac.il)

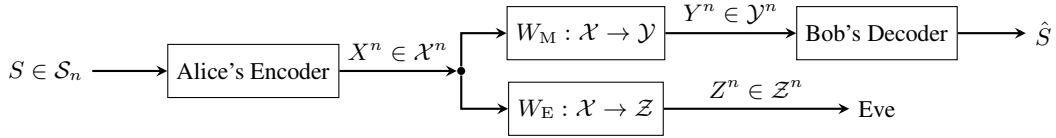


Fig. 1. Wiretap Channel

that are reliable for communication over W_M and guarantee

$$\liminf_{n \rightarrow \infty} -\frac{1}{n} \log I(S; Z^n) \geq \eta. \quad (2)$$

Hayashi [7] was the first to derive a lower bound to the achievable secrecy exponents using the resolvability-based construction of wiretap channel codes from i.i.d. random codes. He, later on, showed that this lower bound can be improved if, on top of a random code sampled from i.i.d. random coding ensemble, a random hash function is used in the construction of the encoder-decoder pair [8]. This technique is known as *privacy amplification*. More recently, it was shown (see special cases of [9, Theorem 2], [10, Theorem 3.1], or the proof given in [11]) that privacy amplification is unnecessary and the exponent derived in [8] lower-bounds the exponential decay rate of the ensemble average of the information leaked to Eve when a wiretap channel code constructed from the ensemble of i.i.d. random codes is used for communication.

To study the *universally achievable* (in the sense defined in [12]) secrecy exponents, constructing codes for wiretap channel from the ensemble of random constant-composition codes is investigated in [13]. A lower bound to the achievable secrecy exponent when this class of wiretap channel codes are used in conjunction with privacy amplification is derived in [13] which is smaller than the lower bound of [8] on the achievable secrecy exponent using i.i.d. random codes.

A. Contribution and Paper Outline

In this paper we first show that the exponent derived via the method of [11] (which was first established in [8]) is indeed the *exact* secrecy exponent for an average code in the ensemble and secondly extend the analysis of [11] to the ensemble of constant-composition random codes (see Theorem 4 and its corollary). This, in particular, implies that the previously-known lower bound to the achievable secrecy exponent using wiretap channel codes constructed from i.i.d. random coding ensemble characterizes the exact exponential decay rate of the average amount of information leaked to the eavesdropper. Moreover, it turns out that the exact secrecy exponent for the wiretap channel codes constructed from constant-composition random codes is larger than the lower bound derived in [13] and there are examples where this dominance is strict. Further, examples show that in general there is no ordering between the secrecy exponents of the ensembles of i.i.d. and constant-composition codes. In other words, for some channels the i.i.d. ensemble yields a better secrecy exponent, whereas in the others, the constant-composition ensemble prevails (see Section IV-B).

The analysis of [11] is based on pure random coding arguments (no privacy amplification is used) and is carried

out by lower-bounding the achievable *resolvability exponents* (see Definition 5) using random codes. We will show, in this work, that this method not only proves the achievability of the exponent, but also, using very similar steps, establishes its exactness (see Definition 6). Moreover, a simple observation shows that the exact resolvability exponent equals the exact secrecy exponent for an ensemble (see Theorem 1), which in turn, allows us to conclude that the exponent derived through this method is the exact secrecy exponent as well.

The remainder of this paper is organized as follows. After setting our notation conventions in Section II, we prove the equivalence of secrecy and resolvability exponents in Section III and reduce the analysis of the exact secrecy exponent for an ensemble to that of the exact resolvability exponent. We present our main result on exact secrecy exponents in Section IV, argue that the exact secrecy exponent for the ensemble of constant-composition random codes is larger than the lower bound derived in [13], and give numerical examples comparing the exponents for two ensembles of i.i.d. and constant-composition random codes. Our main result is proved in Section V. To streamline the presentation, we relegate the straightforward but tedious parts of the proof to the appendices.

B. Related Work

In addition to those cited above, [14] also presents a simple achievability proof for channel resolvability. Based on this proof the authors, in their subsequent work [15], establish strong secrecy for wiretap channel using resolvability-based constructions for wiretap channel codes. The performance of a code for the wiretap channel is measured via two figures of merit, namely, the error probability and information leakage, both of which decay exponentially in block-length when a wiretap channel code sampled from the ensemble of random codes is employed on stationary memoryless channels (as we will also discuss in Theorem 2). The trade-off between secrecy and error exponents (as well as other generalizations of the model) is studied in [16].

Another important problem, in the realm of information-theoretic secrecy, is *secret key agreement* [17], [18]. The secrecy exponents related to this model are studied in [8], [16], [19], [20] and, in particular, in [19], [20] shown to be exact.

II. NOTATION

We use uppercase letters (like X) to denote a random variable and the corresponding lowercase version (x) for a realization of that random variable. The same convention applies to vectors, i.e., $x^n = (x_1, \dots, x_n)$ denotes a realization

of the random vector $X^n = (X_1, \dots, X_n)$. We denote finite sets by script-style uppercase letters like \mathcal{A} . The cardinality of the set \mathcal{A} is denoted by $|\mathcal{A}|$.

We write $f(n) \dot{\leq} g(n)$ if there exists a function $p(n)$ such that $\limsup_{n \rightarrow \infty} \frac{1}{n} \log(p(n)) = 0$ and $f(n) \leq p(n)g(n)$. As noted in [21, p. 2507], when $f(n)$ and $g(n)$ depend on other variables than n it is understood that $p(n)$ can only depend on the *fixed parameters* of the problem such as channel transition probabilities, the cardinality of its input and output alphabet, and its input distribution and not the other parameters f and g may depend on.¹ $f(n) \dot{=} g(n)$ means $f(n) \dot{\leq} g(n)$ and $g(n) \dot{\leq} f(n)$. For $a \in \mathbb{R}$, $[a]^+ \triangleq \max\{a, 0\}$ denotes positive clipping.

We denote the set of distributions on alphabet \mathcal{X} as $\mathcal{P}(\mathcal{X})$. If $P \in \mathcal{P}(\mathcal{X})$, $P^n \in \mathcal{P}(\mathcal{X}^n)$ denotes the product distribution $P^n(x^n) \triangleq \prod_{i=1}^n P(x_i)$ (where x^n denotes the n -dimensional vector $(x_1, \dots, x_n) \in \mathcal{X}^n$). Likewise, if $V: \mathcal{X} \rightarrow \mathcal{Y}$ is a conditional distribution (that is, $\forall x \in \mathcal{X}$, $V(\cdot|x) \in \mathcal{P}(\mathcal{Y})$), $V^n: \mathcal{X}^n \rightarrow \mathcal{Y}^n$ denotes the conditional distribution $V^n(y^n|x^n) = \prod_{i=1}^n V(y_i|x_i)$. For a joint distribution $Q \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})$, Q_X (respectively Q_Y) denotes its x - (respectively y -) marginal. For $P \in \mathcal{P}(\mathcal{X})$ and a stochastic matrix $V: \mathcal{X} \rightarrow \mathcal{Y}$, $P \times V \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})$ denotes the joint distribution $P(x)V(y|x)$ and $P \circ V \in \mathcal{P}(\mathcal{Y})$ denotes the y -marginal of the joint distribution $P \times V$, that is $(P \circ V)(y) = (P \times V)_Y(y) = \sum_x P(x)V(y|x)$.

We denote the *type* of a sequence $x^n \in \mathcal{X}^n$ by $\hat{Q}_{x^n} \in \mathcal{P}(\mathcal{X})$. A distribution $P \in \mathcal{P}(\mathcal{X})$ is an n -*type* if $\forall x \in \mathcal{X}: nP(x) \in \mathbb{Z}$. We denote the set of n -types on \mathcal{X} as $\mathcal{P}_n(\mathcal{X}) \subsetneq \mathcal{P}(\mathcal{X})$ and use the fact that $|\mathcal{P}_n(\mathcal{X})| \leq (n+1)^{|\mathcal{X}|}$ [22, Lemma 2.2] repeatedly. If $P \in \mathcal{P}_n(\mathcal{X})$, we denote the set of all sequences of type P as $\mathcal{T}_P^n \subset \mathcal{X}^n$.

For a distribution $P \in \mathcal{P}(\mathcal{X})$, $\text{supp}(P) \triangleq \{x \in \mathcal{X}: P(x) > 0\}$. If $P, Q \in \mathcal{P}(\mathcal{X})$ are a pair of distributions we say P is absolutely continuous with respect to Q , and denote this by $P \ll Q$, if $\text{supp}(P) \subseteq \text{supp}(Q)$.

The ℓ_1 distance and divergence between two distributions $P, Q \in \mathcal{P}(\mathcal{X})$ are, respectively, defined as

$$|P - Q| \triangleq \sum_{x \in \mathcal{X}} |P(x) - Q(x)| \quad (3)$$

and

$$D(P||Q) \triangleq \sum_{x \in \mathcal{X}} P(x) \log \frac{P(x)}{Q(x)} \quad (4)$$

(here and in the sequel the bases of log and exp are arbitrary but the same). For two stochastic matrices $V: \mathcal{X} \rightarrow \mathcal{Y}$ and $W: \mathcal{X} \rightarrow \mathcal{Y}$, and $P \in \mathcal{P}(\mathcal{X})$, the conditional divergence is defined as

$$D(V||W|P) \triangleq \sum_{x \in \mathcal{X}} P(x) \sum_{y \in \mathcal{Y}} V(y|x) \log \frac{V(y|x)}{W(y|x)} \quad (5)$$

$$= D(P \times V || P \times W). \quad (6)$$

¹Let θ be a parameter that f and g depend on. If $f_\theta(n) \dot{\leq} g_\theta(n)$ then, $\forall \theta$, $\limsup_{n \rightarrow \infty} \frac{1}{n} \log \left(\frac{f_\theta(n)}{g_\theta(n)} \right) \leq 0$ but the reverse is not true. In fact $f_\theta(n) \dot{\leq} g_\theta(n)$ is equivalent to $\limsup_{n \rightarrow \infty} \sup_\theta \frac{1}{n} \log \left(\frac{f_\theta(n)}{g_\theta(n)} \right) \leq 0$ which is a stronger statement than the former.

For $P \in \mathcal{P}(\mathcal{X})$,

$$H(P) \triangleq - \sum_{x \in \mathcal{X}} P(x) \log P(x). \quad (7)$$

For $Q \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})$, $I(Q) \triangleq D(Q || Q_X \times Q_Y)$. If $P \in \mathcal{P}(\mathcal{X})$ and $V: \mathcal{X} \rightarrow \mathcal{Y}$ is a stochastic matrix, $I(P, V) \triangleq I(P \times V)$ denotes the mutual information developed across the channel V with input distribution P .

III. SECRECY VIA CHANNEL RESOLVABILITY

As we mentioned earlier, *channel resolvability* is a convenient and powerful tool for the analysis of secrecy [4], [5]. The concept of resolvability dates back to Wyner [23], where he observed that, given a stationary memoryless channel $W: \mathcal{X} \rightarrow \mathcal{Z}$ and an input distribution P_X that induces the distribution $P_Z = P_X \circ W$ at its output, it is possible to well-approximate the product distribution P_Z^n at the output of W^n (the product channel corresponding to n independent uses of W) by transmitting a uniformly chosen codeword from a code of rate $R > I(X; Z)$. Indeed, if the code is sampled from the i.i.d. random coding ensemble, with very high probability the normalized divergence between the channel output distribution and P_Z^n can be made arbitrarily small by choosing n sufficiently large. Han and Verdú [24] and Hayashi [7] developed this theory further by replacing the measure of approximation by normalized ℓ_1 distance and unnormalized divergence, respectively, and showed first, that the same limits on the code size hold in these cases and, second, that the distance between the output distribution and the target distribution P_Z^n vanishes exponentially fast as the block-length increases (similar results are derived in [11], [14], [25] as well). In particular, in [7], [10], [11], [15], the exponential decay of the informational divergence is leveraged to establish an exponentially decaying upper bound on the information leaked to the eavesdropper in wiretap channel's model.

We can extend the notion of resolvability and ask for the approximation of arbitrary target distributions. Given a code $\mathcal{C}_n = \{x_1^n, \dots, x_M^n\}$ (of block-length n and size M) and the channel $W: \mathcal{X} \rightarrow \mathcal{Z}$, denote by $P_{\mathcal{C}_n}$ the output distribution of W^n when a uniformly chosen codeword from \mathcal{C}_n is transmitted, that is,

$$P_{\mathcal{C}_n}(z^n) \triangleq \frac{1}{M} \sum_{i=1}^M W^n(z^n|x_i^n). \quad (8)$$

Definition 2. Given a stationary memoryless channel $W: \mathcal{X} \rightarrow \mathcal{Z}$, a rate R , and a sequence of target distributions $\Phi = \{\Phi_n \in \mathcal{P}(\mathcal{Z}^n)\}_{n \in \mathbb{N}}$, a number $E^\Phi(W, R)$ is an achievable *resolvability exponent* over the channel W , at rate R , with respect to Φ if there exists a sequence $\{\mathcal{C}_n\}_{n \in \mathbb{N}}$ of codes (\mathcal{C}_n of block-length n), such that $\limsup_{n \rightarrow \infty} \frac{1}{n} \log |\mathcal{C}_n| \leq R$ and

$$\liminf_{n \rightarrow \infty} -\frac{1}{n} \log D(P_{\mathcal{C}_n} || \Phi_n) \geq E^\Phi(W, R). \quad (9)$$

Definition 3. The supremum of all achievable resolvability exponents over $W: \mathcal{X} \rightarrow \mathcal{Z}$, at rate R , with respect to $\Phi = \{\Phi_n \in \mathcal{P}(\mathcal{Z}^n)\}_{n \in \mathbb{N}}$ is the resolvability exponent of the channel $W: \mathcal{X} \rightarrow \mathcal{Z}$ at rate R with respect to Φ .

Computing “the” resolvability exponent is a difficult task as it necessitates a search over all possible sequences of codes to find the best resolvability code. The usual way to circumvent such a difficulty is to use the probabilistic method and analyze the achievable exponents for an ensemble of random codes.

Definition 4. Given $\Pi = \{P_{X^n} \in \mathcal{P}(\mathcal{X}^n)\}_{n \in \mathbb{N}}$, a sequence of probability distributions on \mathcal{X}^n , an *ensemble of random codes* of rate (at most) R is a sequence of random codes \mathcal{C}_n of block-length n and size $M = \lfloor \exp(nR) \rfloor$ obtained by sampling the codewords independently from the distribution P_{X^n} . In other words,

$$\Pr\{\mathcal{C}_n = \{x_1^n, \dots, x_M^n\}\} = \prod_{i=1}^M P_{X^n}(x_i^n). \quad (10)$$

Definition 5. Given $\Pi = \{P_{X^n} \in \mathcal{P}(\mathcal{X}^n)\}_{n \in \mathbb{N}}$, a stationary memoryless channel $W: \mathcal{X} \rightarrow \mathcal{Z}$, and a rate R , a number $\underline{E}_s(\Pi, W, R)$ is an achievable resolvability exponent for the ensemble of random codes of rate (at most) R defined by Π , over the channel W , if

$$\liminf_{n \rightarrow \infty} -\frac{1}{n} \log \mathbb{E}[D(P_{\mathcal{C}_n} \| \bar{P}_{Z^n})] \geq \underline{E}_s(\Pi, W, R), \quad (11)$$

where \mathcal{C}_n is a random code of size $M = \lfloor \exp(nR) \rfloor$ distributed according to (10) and the sequence of target distributions $\{\bar{P}_{Z^n} \in \mathcal{P}(\mathcal{Z}^n)\}_{n \in \mathbb{N}}$ is defined as

$$\bar{P}_{Z^n}(z^n) \triangleq (P_{X^n} \circ W^n)(z^n) = \sum_{x^n \in \mathcal{X}^n} P_{X^n}(x^n) W^n(z^n | x^n). \quad (12)$$

Remark. In the passage to the probabilistic method, we restricted the sequence of target measures to those induced by the code sampling distribution P_{X^n} at the output of the n -fold use of W , (12). Indeed, it is easy to verify that when \mathcal{C}_n is a random code whose codewords are drawn independently from P_{X^n} , for any distribution $\Phi_n \in \mathcal{P}(\mathcal{Z}^n)$,

$$\mathbb{E}[D(P_{\mathcal{C}_n} \| \Phi_n)] = \mathbb{E}[D(P_{\mathcal{C}_n} \| \bar{P}_{Z^n})] + D(\bar{P}_{Z^n} \| \Phi_n). \quad (13)$$

Therefore, to show the existence of good resolvability codes for approximating a sequence of target distributions $\{\Phi_n \in \mathcal{P}(\mathcal{Z}^n)\}_{n \in \mathbb{N}}$ via random coding arguments, we can exclusively consider the ensembles of random codes whose sampling distribution P_{X^n} induces Φ_n at the output of W^n —any other ensemble is *suboptimal* due to the residual divergence $D(\bar{P}_{Z^n} \| \Phi_n)$.

Definition 6. The *exact* resolvability exponent of the ensemble of random codes of rate (at most) R defined via the sequence of distributions $\Pi = \{P_{X^n} \in \mathcal{P}(\mathcal{X}^n)\}_{n \in \mathbb{N}}$, over the channel $W: \mathcal{X} \rightarrow \mathcal{Z}$, is defined as

$$E_s(\Pi, W, R) \triangleq \lim_{n \rightarrow \infty} -\frac{1}{n} \log \mathbb{E}[D(P_{\mathcal{C}_n} \| \bar{P}_{Z^n})] \quad (14)$$

(where $\bar{P}_{Z^n} \triangleq P_{X^n} \circ W^n$) provided that the limit exists.

For the sake of completeness, let us also formally define the error exponent for an ensemble of random codes.

Definition 7. Given $\Pi = \{P_{X^n} \in \mathcal{P}(\mathcal{X}^n)\}_{n \in \mathbb{N}}$, a stationary memoryless channel $W: \mathcal{X} \rightarrow \mathcal{Y}$, and a rate R , a number

$\underline{E}_r(\Pi, W, R)$ is called an achievable *error exponent* of the ensemble Π at rate R on channel W , if

$$\liminf_{n \rightarrow \infty} -\frac{1}{n} \log \mathbb{E}[\Pr\{\hat{s}_{\text{ML}}(Y^n) \neq S\}] \geq \underline{E}_r(\Pi, W, R) \quad (15)$$

when \mathcal{C}_n , a random code of size $M = \lfloor \exp(nR) \rfloor$ is used to communicate a uniformly chosen message $S \in \{1, 2, \dots, M\}$ via n independent uses of W , y^n is the output sequence of W^n , and $\hat{s}_{\text{ML}}(y^n)$ is the ML estimation of S given y^n .

Remark. For the ensembles of interest in this paper, i.e., the ensembles of i.i.d. and constant-composition random codes the exact error exponents are well-known [22], [26], [27]. (The exactness of the random exponent of [22, Theorem 10.2] follows from exponential tightness of the truncated union bound [28, Appendix A].)

Definition 8. Given a sequence distributions $\Pi = \{P_{X^n} \in \mathcal{P}(\mathcal{X}^n)\}_{n \in \mathbb{N}}$, and a pair of secret message and *random binning* rates (R_s, R) a random *wiretap channel code* is obtained by partitioning a random code of size $\lfloor \exp[n(R_s + R)] \rfloor$ in the ensemble of random codes defined via Π into $M_s \doteq \exp(nR_s)$ sub-codes (or bins) of size $\lfloor \exp(nR) \rfloor$, denoted as \mathcal{C}_n^s , $s \in \{1, 2, \dots, M_s\}$, each associated to a message. To communicate the message s , the encoder transmits a codeword from the sub-code \mathcal{C}_n^s uniformly at random (thus it requires an entropy rate of R).

Theorem 1. Let $W_M: \mathcal{X} \rightarrow \mathcal{Y}$ and $W_E: \mathcal{X} \rightarrow \mathcal{Z}$ be the pair of legitimate receiver's and wiretapper's stationary memoryless channels respectively (see Figure 1). Fix a sequence of codeword sampling distributions $\Pi = \{P_{X^n} \in \mathcal{P}(\mathcal{X}^n)\}_{n \in \mathbb{N}}$. Let $\underline{E}_r(\Pi, W_M, R)$ be an achievable error exponent for the ensemble Π over the channel W_M at rate R (see Definition 7) and $E_s(\Pi, W_E, R)$ be the exact resolvability exponent of the ensemble Π over the channel W_E at rate R (see Definition 6). Then for any rate pair (R_s, R) such that $E_s(\Pi, W_E, R + R_s) > E_s(\Pi, W_E, R)$, using the ensemble of random wiretap channel codes constructed as in Definition 8, when the secret message S is uniformly distributed,

$$\liminf_{n \rightarrow \infty} -\frac{1}{n} \log \mathbb{E}[\Pr\{\hat{s}_{\text{ML}}(Y^n) \neq S\}] \geq \underline{E}_r(\Pi, W_M, R + R_s) \quad (16)$$

$$\lim_{n \rightarrow \infty} -\frac{1}{n} \log \mathbb{E}[I(S; Z^n)] = E_s(\Pi, W_E, R), \quad (17)$$

where $\hat{s}_{\text{ML}}(y^n)$ is the ML estimation of the sent message given y^n , the output of legitimate receiver's channel. In other words, E_s (evaluated at the random binning rate R) is also the exact secrecy exponent for the ensemble Π .

Proof: That $\underline{E}_r(\Pi, W_M, R + R_s)$ is an achievable error exponent for the legitimate receiver is obvious: probability of misdecoding the message S is upper-bounded by probability of incorrect decoding of the sent codeword. We shall, hence, only prove (17).

Since, to communicate a particular message $s \in \mathcal{S}_n$, the encoder transmits a codeword from the code \mathcal{C}_n^s associated to the message s , conditioned on $S = s$ the output of W_E^n has distribution $P_{\mathcal{C}_n^s}$ and, since S is uniformly distributed,

the *unconditional* output distribution of $W_{\mathbf{E}}^n$ will be P_{C_n} (cf. (8)). Therefore, the identity $I(A; B) = D(P_{B|A} \| Q_B | P_A) - D(P_B \| Q_B)$ (for $(A, B) \sim P_{AB}$ and any arbitrary distribution Q_B) yields:

$$\mathbb{E}[I(S; Z^n)] = \mathbb{E}[D(P_{C_n^s} \| \bar{P}_{Z^n} | P_S)] - \mathbb{E}[D(P_{C_n} \| \bar{P}_{Z^n})]. \quad (18)$$

Using the linearity of expectation and the fact that the sub-codes C_n^s are identically distributed we get:

$$\begin{aligned} \mathbb{E}[D(P_{C_n^s} \| \bar{P}_{Z^n} | P_S)] &= \sum_{s=1}^{M_s} P_S(s) \mathbb{E}[D(P_{C_n^s} \| \bar{P}_{Z^n})] \\ &= \mathbb{E}[D(P_{C_n^1} \| \bar{P}_{Z^n})]. \end{aligned} \quad (19)$$

Thus, by (14), we have

$$\begin{aligned} \lim_{n \rightarrow \infty} -\frac{1}{n} \log \mathbb{E}[D(P_{C_n^s} \| \bar{P}_{Z^n} | P_S)] &= E_s(\Pi, W_{\mathbf{E}}, R), \quad (20) \\ \lim_{n \rightarrow \infty} -\frac{1}{n} \log \mathbb{E}[D(P_{C_n} \| \bar{P}_{Z^n})] &= E_s(\Pi, W_{\mathbf{E}}, R + R_s) \\ &> E_s(\Pi, W_{\mathbf{E}}, R). \end{aligned} \quad (21)$$

where the last inequality follows from the assumption that $E_s(\Pi, W_{\mathbf{E}}, R + R_s) > E_s(\Pi, W_{\mathbf{E}}, R)$. Using (20) and (21) in (18) concludes the proof. ■

Remark 1. That (a lower bound to) the resolvability exponent, lower-bounds the secrecy exponent is already used in [7], [10], [11]. Theorem 1 complements this result by showing that the exact resolvability exponent equals the exact secrecy exponent.

Remark 2. To show the achievability of \underline{E}_r in the proof of Theorem 1, we used a decoder that estimates the sent codeword and then decides to which sub-code it belongs. In [29] it has been shown that, when the code sampling distribution P_{X^n} depends on x^n only through its type, the error exponent of this decoder is the same as that of the *optimal* decoder (that computes the likelihood score for each message s by summing up the likelihoods of all codewords in C_n^s and then decides on the most likely message) for an average code in the ensemble.

Remark 3. Equations (16) and (17) suggest a trade-off in code design in terms of the choice of input distributions, $\Pi = \{P_{X^n} \in \mathcal{P}(\mathcal{X}^n)\}_{n \in \mathbb{N}}$. The sequence of input distributions Π that maximizes E_s may not coincide with the one that maximizes \underline{E}_r .

Theorem 1 reduces the problem of computing the exact secrecy exponent of the ensemble to that of computing the exact resolvability exponent of the ensemble which is easier as the former involves the divergence between two random distributions $P_{C_n^s}$ and P_{C_n} while the latter depends only on $P_{C_n^s}$. The assumption on uniform prior of secret messages is crucial to establish such a result.² However, in a practical system, the user chooses the distribution of the secret messages and it is desirable to have a worst-case guarantee of performance. Therefore, before continuing with the main results of the paper, it is worth mentioning the following result (which is proved in Appendix A).

²Without such an assumption $I(S; Z^n) = 0$, namely, the secrecy exponent is infinity if P_S is positive only for a single secret message.

Theorem 2. Let $W_{\mathbf{M}}: \mathcal{X} \rightarrow \mathcal{Y}$ and $W_{\mathbf{E}}: \mathcal{X} \rightarrow \mathcal{Z}$ be the pair of legitimate receiver's and wiretapper's stationary memoryless channels respectively (see Figure 1) and $\Pi = \{P_{X^n} \in \mathcal{P}(\mathcal{X}^n)\}_{n \in \mathbb{N}}$ be a sequence of code sampling distributions. If $\underline{E}_r(\Pi, W_{\mathbf{M}}, R)$ is an achievable error exponent for the ensemble Π over the channel $W_{\mathbf{M}}$ at rate R that is continuous in R and $\underline{E}_s(\Pi, W_{\mathbf{E}}, R)$ is an achievable resolvability exponent of the ensemble Π over the channel $W_{\mathbf{E}}$, then there exists a sequence of wiretap channel codes of secret message R_s and random binning rate R in the ensemble (indexed by their block-length n) using which,

$$\liminf_{n \rightarrow \infty} -\frac{1}{n} \log \Pr\{\hat{s}_{\text{ML}}(Y^n) \neq S\} \geq \underline{E}_r(\Pi, W_{\mathbf{M}}, R + R_s), \quad (22)$$

$$\liminf_{n \rightarrow \infty} -\frac{1}{n} \log I(S; Z^n) \geq \underline{E}_s(\Pi, W_{\mathbf{E}}, R) \quad (23)$$

for any distribution of the secret message P_S .

IV. EXACT RESOLVABILITY EXPONENTS

In light of Theorem 1, we shall focus on deriving the exact resolvability exponents for the ensembles of i.i.d. and constant-composition random codes. Accordingly, C_n will denote the random resolvability code in this section and not the entire wiretap channel code.

A. Main Result

Theorem 3. Let C_n be a random code of block-length n and rate R constructed by sampling $M = \lfloor \exp(nR) \rfloor$ codewords independently from the distribution $P_{X^n} \in \mathcal{P}(\mathcal{X}^n)$ (see (10)). Let $W: \mathcal{X} \rightarrow \mathcal{Z}$ be a discrete memoryless channel and P_{C_n} be the (random) output distribution of W^n when a uniformly chosen codeword from C_n is transmitted via n independent uses of W (see (8)). Then,

(i) if $P_{X^n} = P_X^n$ for some $P_X \in \mathcal{P}(\mathcal{X})$,

$$\begin{aligned} \mathbb{E}[D(P_{C_n} \| \bar{P}_{Z^n})] &= \begin{cases} \exp(-nE_{s,n}^{\text{i.i.d.}}(P_X, W, R)) & \text{if } I(P_X, W) > 0, \\ 0 & \text{if } I(P_X, W) = 0, \end{cases} \end{aligned} \quad (24)$$

where

$$\begin{aligned} E_{s,n}^{\text{i.i.d.}}(P_X, W, R) &= \min_{Q \in \mathcal{P}_n(\mathcal{X} \times \mathcal{Z})} \{D(Q \| P_X \times W) \\ &\quad + [R - f(Q \| P_X \times W)]^+\}, \end{aligned} \quad (25a)$$

with

$$f(Q \| Q') \triangleq \sum_{(x,z) \in \mathcal{X} \times \mathcal{Z}} Q(x,z) \log \frac{Q'(x,z)}{Q'_X(x)Q'_Z(z)}, \quad (25b)$$

for any two distributions $Q, Q' \in \mathcal{P}(\mathcal{X} \times \mathcal{Z})$;

- (ii) if $P_{X^n}(x^n) = \mathbb{1}\{x^n \in \mathcal{T}_{P_n}^n\} / |\mathcal{T}_{P_n}^n|$ for some sequence of n -types $\{P_n \in \mathcal{P}_n(\mathcal{X})\}_{n \in \mathbb{N}}$ that converge to $P_X \in \mathcal{P}(\mathcal{X})$, i.e., $\lim_{n \rightarrow \infty} |P_n - P_X| = 0$,

$$\mathbb{E}[D(P_{C_n} \| \bar{P}_{Z^n})] \doteq \begin{cases} \exp(-nE_{s,n}^{\text{c.c.}}(P_n, W, R)) & \text{if } I(P_X, W) > 0, \\ 0 & \text{if } I(P_X, W) = 0, \end{cases} \quad (26)$$

where

$$E_{s,n}^{\text{c.c.}}(P_n, W, R) = \min_{P_n \times V \in \mathcal{P}_n(\mathcal{X} \times \mathcal{Z})} \left\{ D(V \| W | P_n) + [R - g_n(V \| W | P_n)]^+ \right\}, \quad (27a)$$

with

$$g_n(V \| W | P) \triangleq \omega(V \| W | P) + H(P \circ V) + \min_{\substack{V': \mathcal{X} \rightarrow \mathcal{Z}: \\ P \times V' \in \mathcal{P}_n(\mathcal{X} \times \mathcal{Z}), \\ P \circ V' = P \circ V}} D(V' \| W | P), \quad (27b)$$

and

$$\omega(V \| W | P) \triangleq \sum_{(x,z) \in \mathcal{X} \times \mathcal{Z}} P(x) V(z|x) \log W(z|x), \quad (27c)$$

for any distribution $P \in \mathcal{P}(\mathcal{X})$ and pair of stochastic matrices $V: \mathcal{X} \rightarrow \mathcal{Z}$ and $W: \mathcal{X} \rightarrow \mathcal{Z}$.

Recall that in the above $\bar{P}_{Z^n} = P_{X^n} \circ W^n$ (see (12)).

Theorem 3 gives exponentially tight bounds on the expected divergence between the output distribution of W^n , when its input is a uniformly chosen codeword from a randomly chosen code and the distribution induced by the code sampling distribution at any finite (but possibly large) block-length n . As a consequence, the exact exponential decay rate of the aforementioned divergence, namely the exact resolvability exponent for the ensembles of interest, is the limit of the exponents of (24) and (26) as n goes to infinity. The exact resolvability exponents have the same forms as (25) and (27) except that the search space of the minimizations will change from the grid of empirical distributions to the set of all distributions.

Theorem 4.

- (i) For the sequence of i.i.d. random codes of rate R , i.e., those defined via the sequence of sampling distributions $\{P_{X^n} = P_X^n\}_{n \in \mathbb{N}}$ for some $P_X \in \mathcal{P}(\mathcal{X})$,

$$\lim_{n \rightarrow \infty} -\frac{1}{n} \log(\mathbb{E}[D(P_{C_n} \| \bar{P}_{Z^n})]) = \begin{cases} E_s^{\text{i.i.d.}}(P_X, W, R) & \text{if } I(P_X, W) > 0, \\ +\infty & \text{if } I(P_X, W) = 0, \end{cases} \quad (28)$$

where

$$E_s^{\text{i.i.d.}}(P_X, W, R) = \min_{Q \in \mathcal{P}(\mathcal{X} \times \mathcal{Z})} \left\{ D(Q \| P_X \times W) + [R - f(Q \| P_X \times W)]^+ \right\}, \quad (29)$$

and f is defined in (25b).

- (ii) For the sequence of constant-composition random codes of rate R , i.e., those defined via the sequence of sampling distributions $\{P_{X^n} = \mathbb{1}\{x^n \in \mathcal{T}_{P_n}^n\} / |\mathcal{T}_{P_n}^n|\}_{n \in \mathbb{N}}$ for some sequence of n -types $\{P_n \in \mathcal{P}_n(\mathcal{X})\}_{n \in \mathbb{N}}$ that converge to P_X , namely, $\lim_{n \rightarrow \infty} |P_n - P_X| = 0$,

$$\lim_{n \rightarrow \infty} -\frac{1}{n} \log(\mathbb{E}[D(P_{C_n} \| \bar{P}_{Z^n})]) = \begin{cases} E_s^{\text{c.c.}}(P_X, W, R) & \text{if } I(P_X, W) > 0, \\ +\infty & \text{if } I(P_X, W) = 0, \end{cases} \quad (30)$$

where

$$E_s^{\text{c.c.}}(P_X, W, R) = \min_{V: \mathcal{X} \rightarrow \mathcal{Z}} \left\{ D(V \| W | P_X) + [R - g(V \| W | P_X)]^+ \right\}, \quad (31a)$$

with

$$g(V \| W | P) \triangleq \omega(V \| W | P) + H(P \circ V) + \min_{\substack{V': \mathcal{X} \rightarrow \mathcal{Z}: \\ P \circ V' = P \circ V}} D(V' \| W | P), \quad (31b)$$

for any distribution $P \in \mathcal{P}(\mathcal{X})$ and pair of stochastic matrices $V: \mathcal{X} \rightarrow \mathcal{Z}$ and $W: \mathcal{X} \rightarrow \mathcal{Z}$ (and ω defined as in (27c)).

Both exponents $E_s^{\text{i.i.d.}}$ and $E_s^{\text{c.c.}}$ are positive and strictly increasing in R for $R > I(P_X, W)$. Moreover, the value of $E_s^{\text{i.i.d.}}$ can be computed through

$$E_s^{\text{i.i.d.}}(P_X, W, R) = \max_{0 \leq \lambda \leq 1} \{\lambda R - F_0(P_X, W, \lambda)\} \quad (32a)$$

with

$$F_0(P_X, W, \lambda) \triangleq \log \sum_{(x,z) \in \mathcal{X} \times \mathcal{Z}} P_X(x) W(z|x)^{1+\lambda} (P_X \circ W)(z)^{-\lambda}. \quad (32b)$$

Theorem 4 is proved in Appendix B.

Corollary 5. The exponents $E_s^{\text{i.i.d.}}(P_X, W_E, R)$ and $E_s^{\text{c.c.}}(P_X, W_E, R)$ of (29) and (31) are the exact secrecy exponents for the ensembles of random wiretap channel codes of rate pair (R, R_s) constructed from the ensembles of random i.i.d. and constant-composition codes, respectively, provided that $R_s > 0$ and $R > I(P_X, W_E)$.

B. Comparison of Exponents

Corollary 5 states that the exponent $E_s^{\text{i.i.d.}}$, which was already derived in [8], [10], [11] is, indeed, the exact secrecy exponent for the ensemble of i.i.d. random codes. (The exponent is expressed in the form of (32) in [8], [10], [11].) In contrast, it can be shown that $E_s^{\text{c.c.}}$, the exact secrecy exponent for the ensemble of constant-composition random codes, is larger than the previously-derived lower bound in [13]:

$$\underline{E}_s(P_X, W_E, R) = \max_{0 \leq \lambda \leq 1} \{\lambda R - E_0(P_X, W_E, \lambda)\}, \quad (33a)$$

with

$$E_0(P_X, W, \lambda) \triangleq \log \sum_{z \in \mathcal{Z}} \left(\sum_{x \in \mathcal{X}} P_X(x) W(z|x)^{\frac{1}{1-\lambda}} \right)^{1-\lambda}. \quad (33b)$$

(Note that the function E_0 in (33b) is essentially Gallager's E_0 [26] up to a minus sign.) For every discrete memoryless stationary channel $W: \mathcal{X} \rightarrow \mathcal{Z}$,

$$E_s^{c.c.}(P_X, W, R) \geq \underline{E}_s(P_X, W, R). \quad (34)$$

This follows from the fact that $g(V\|W|P) \leq I(P, V)$ using similar steps as in [22, Problem 10.24] to derive Gallager-style expressions of error exponents (see Appendix C for a complete proof).

As for comparing the secrecy exponents $E_s^{i.i.d.}$ and $E_s^{c.c.}$, numerical examples show that in general, there is no ordering between them. In particular, as shown in Figures 2 and 3, for the binary symmetric channel and the binary erasure channel, the ensemble of constant-composition random codes leads to a larger exponent than the ensemble of i.i.d. random codes. The two exponents are equal when the input distribution is uniform. On the other side, in Figures 4 and 5, we see that for asymmetric channels (the Z-channel and the binary asymmetric channel) the ensemble of constant-composition random codes results in a smaller secrecy exponent compared to the ensemble of i.i.d. random codes. The reader may find details on how the exponents are computed in Appendix D.

V. PROOF OF THEOREM 3

In this section, we fix P_X and set $P_{XZ}(x, z) = P_X(x)W(z|x)$. Moreover, we assume, without essential loss of generality, that (i) $\text{supp}(P_X) = \mathcal{X}$ (and for the constant-composition codes, $\forall n, \text{supp}(P_n) = \mathcal{X}$), and (ii) for every $z \in \mathcal{Z}$, there exists at least one $x \in \mathcal{X}$ such that $W(z|x) > 0$.

Recall that the setting we are considering is as follows: A random code $C_n = \{X_1^n, \dots, X_M^n\}$ of block-length n and size $M = \lfloor \exp(nR) \rfloor$ is constructed by sampling each codeword independently from distribution P_{X^n} . A uniformly chosen codeword from this code is transmitted through the product channel W^n and the (random) distribution of its output sequence is as in (8).

Trivial Case (zero-capacity channel): If P_X is such that $I(X; Z) = 0$, then $\forall x \in \mathcal{X}$ and $\forall z \in \mathcal{Z}$, $W(z|x) = P_Z(z)$. This implies that for any code C_n , $P_{C_n} = P_Z^n$. Moreover, $\bar{P}_{Z^n} = P_{X^n} \circ W^n = P_Z^n$ as well, thus, $D(P_{C_n} \| \bar{P}_{Z^n}) = 0$ (with probability 1 for a random code) which, in turn, implies $\mathbb{E}[D(P_{C_n} \| \bar{P}_{Z^n})] = 0$.

Now, we begin the non-trivial part of the proof, namely when the channel output sequence Z^n is correlated with its input. For any fixed $z^n \in \mathcal{Z}^n$, $P_{C_n}(z^n)$ is an average of M i.i.d. random variables $W^n(z^n|X_i^n)$, $i = 1, \dots, M$ and, hence, is naturally expected to concentrate around its mean, which is exactly $\bar{P}_{Z^n}(z^n)$. However, since the distribution of each of summands in (8) depends on n , a plain application of law of large numbers is not possible in this setting. Let

$$L(z^n) \triangleq \begin{cases} \frac{P_{C_n}(z^n)}{\bar{P}_{Z^n}(z^n)} & \text{if } \bar{P}_{Z^n}(z^n) > 0, \\ 1 & \text{otherwise,} \end{cases} \quad (35)$$

denote the (random) likelihood ratio of each sequence $z^n \in \mathcal{Z}^n$. By construction,

$$\mathbb{E}[L(z^n)] = 1, \quad \forall z^n \in \mathcal{Z}^n. \quad (36)$$

Moreover, it follows that $P_{C_n} \ll \bar{P}_{Z^n}$ with probability 1 (see Lemma 6). Thus, the linearity of expectation yields

$$\mathbb{E}[D(P_{C_n} \| \bar{P}_{Z^n})] = \mathbb{E} \left[\sum_{z^n \in \mathcal{Z}^n} P_{C_n}(z^n) \log \left(\frac{P_{C_n}(z^n)}{\bar{P}_{Z^n}(z^n)} \right) \right] \quad (37)$$

$$= \sum_{z^n \in \mathcal{Z}^n} \mathbb{E} \left[P_{C_n}(z^n) \log \left(\frac{P_{C_n}(z^n)}{\bar{P}_{Z^n}(z^n)} \right) \right] \quad (38)$$

$$= \sum_{z^n \in \mathcal{Z}^n} \bar{P}_{Z^n}(z^n) \mathbb{E}[L(z^n) \log L(z^n)] \quad (39)$$

To prove Theorem 3 we derive exponentially tight bounds on the value of $\mathbb{E}[L(z^n) \log L(z^n)]$ (for each individual $z^n \in \mathcal{Z}^n$) and eventually combine those bounds in (39) to derive the exponents of Theorem 3.

A. Preliminaries

Lemma 6. *Let \bar{P}_{Z^n} be as defined in (12). Then:*

- (i) $P_{C_n} \ll \bar{P}_{Z^n}$ with probability 1.
- (ii) For any codeword sampling distribution $P_{X^n} \in \mathcal{P}(\mathcal{X}^n)$ that depends on x^n only through its type, $\bar{P}_{Z^n}(z^n)$ will depend on z^n only through its type.
- (iii) For both choices of P_{X^n} in Theorem 3, $\forall z^n \in \text{supp}(\bar{P}_{Z^n})$, $\bar{P}_{Z^n}(z^n) > (1/\alpha)^n$ where

$$\alpha \triangleq \begin{cases} \frac{1}{P_{\min} W_{\min}} & \text{if } P_{X^n} = P_X^n, \\ \frac{|\mathcal{X}|}{W_{\min}} & \text{if } P_{X^n} = \frac{\mathbb{1}_{\{x^n \in \mathcal{T}_{P_n}^n\}}}{|\mathcal{T}_{P_n}^n|}, \end{cases} \quad (40)$$

with $P_{\min} \triangleq \min_{x \in \mathcal{X}} P_X(x)$ and $W_{\min} \triangleq \min_{(x,z) \in \mathcal{X} \times \mathcal{Z}: W(z|x) > 0} W(z|x)$.

Proof: See Appendix E. ■

Remark. For the i.i.d. random coding ensemble, i.e., when $P_{X^n} = P_X^n$, the reference measure \bar{P}_{Z^n} equals the product measure P_Z^n and, hence, $\text{supp}(\bar{P}_{Z^n}) = \mathcal{Z}^n$ (since we assumed $\text{supp}(P_X) = \mathcal{X}$ and for every $z \in \mathcal{Z}$ there exists at least one $x \in \mathcal{X}$ such that $W(z|x) > 0$). In contrast, when P_{X^n} is the uniform distribution over the type-class $\mathcal{T}_{P_n}^n$ (i.e., for the constant-composition random coding ensemble) the support of \bar{P}_{Z^n} need not necessarily be \mathcal{Z}^n . For instance, consider a binary erasure channel and P_n being uniform distribution on $\{0, 1\}$ (for even n). Then \bar{P}_{Z^n} puts no mass on the all-zero output sequence, and by symmetry, neither on the all-one sequence.

Lemma 7. *Let A be an arbitrary non-negative random variable. Then, for any $\theta > 0$,*

$$c(\theta) \left[\frac{\text{var}(A)}{\mathbb{E}[A]} - \tau_\theta(A) \right] \leq \mathbb{E} \left[A \ln \left(\frac{A}{\mathbb{E}[A]} \right) \right] \leq \frac{\text{var}(A)}{\mathbb{E}[A]} \quad (41)$$

where

$$\tau_\theta(A) \triangleq \mathbb{E}[A] \left[\theta^2 \Pr\{A > (\theta + 1) \mathbb{E}[A]\} + 2 \int_\theta^{+\infty} v \Pr\{A > (v + 1) \mathbb{E}[A]\} dv \right], \quad (42)$$

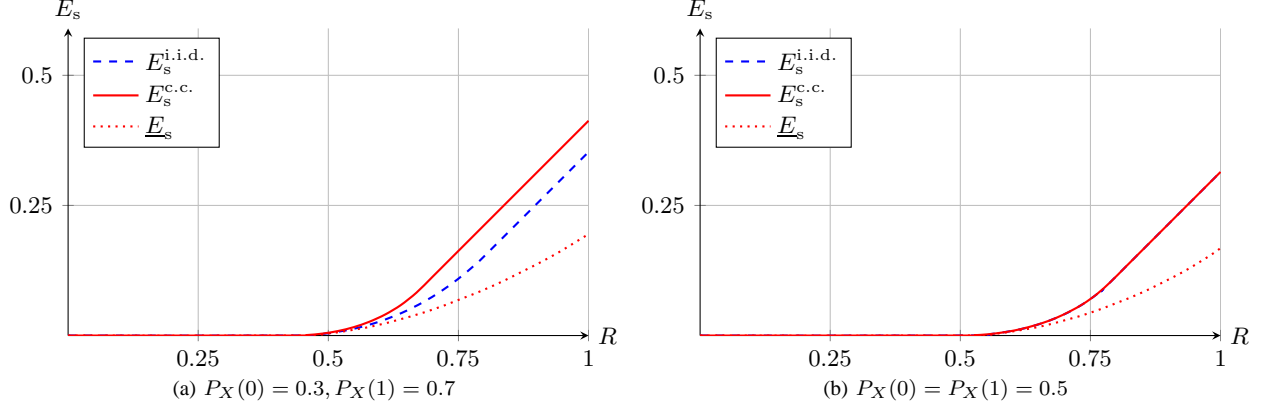


Fig. 2. Comparison of secrecy exponents for Binary Symmetric Channel with crossover probability 0.11

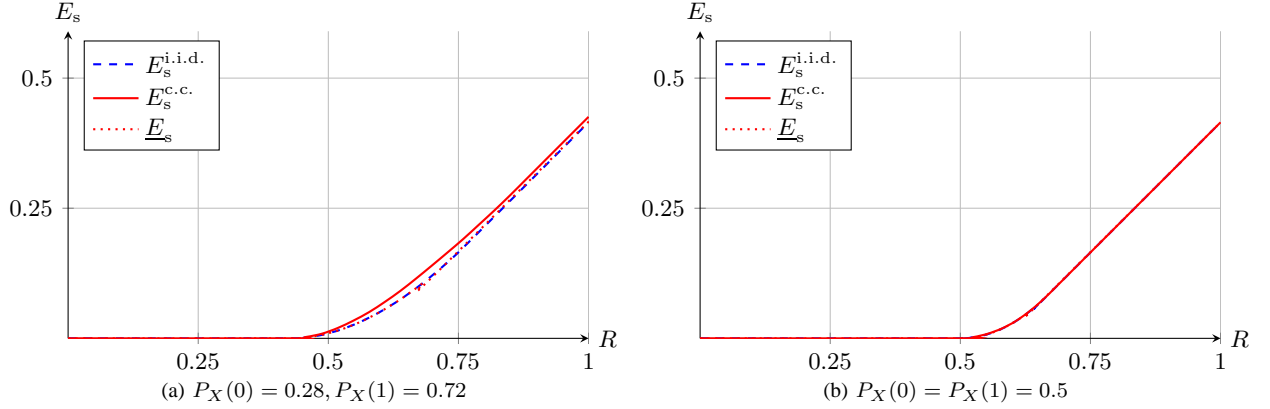


Fig. 3. Comparison of secrecy exponents for Binary Erasure Channel with erasure probability 0.5

and

$$c(\theta) \triangleq \frac{(1+\theta)\ln(1+\theta) - \theta}{\theta^2}. \quad (43)$$

Proof: See Appendix F. ■

Remark. It follows from Jensen's inequality that $\mathbb{E}[A \ln(A/\mathbb{E}[A])] \geq 0$. Lemma 7 improves this lower bound for random variables with sufficiently small tails.

Unfortunately, $L(z^n)$ has heavy tails and a direct application of Lemma 7 to $L(z^n)$ will not result in exponentially tight bounds on $\mathbb{E}[L(z^n) \log L(z^n)]$. However, it turns out that $L(z^n)$ can be split into light- and heavy-tail components. As we shall see shortly, the heavy-tail component contributes to $\mathbb{E}[L(z^n) \log L(z^n)]$ only via its mean and Lemma 7 can be applied to the light-tail component to obtain exponentially tight bounds on $\mathbb{E}[L(z^n) \log L(z^n)]$.

Since $\bar{P}_{Z^n}(z^n)$ depends on z^n only through its type, we can use type enumeration method [29], [30] and write

$$L(z^n) = \frac{1}{M} \sum_{i=1}^M \frac{W^n(z^n | X_i^n)}{\bar{P}_{Z^n}(z^n)} \quad (44)$$

$$= \frac{1}{M} \sum_{Q \in \mathcal{P}_n(\mathcal{X} \times \mathcal{Z})} N_Q(z^n) \ell(Q) \quad (45)$$

where

$$\ell(Q) \triangleq \frac{W^n(\tilde{z}^n | \tilde{x}^n)}{\bar{P}_{Z^n}(\tilde{z}^n)} \quad \text{for some } (\tilde{x}^n, \tilde{z}^n) \in \mathcal{T}_Q^n, \quad (46)$$

and

$$N_Q(z^n) \triangleq |\{x^n \in \mathcal{C}_n : (x^n, z^n) \in \mathcal{T}_Q^n\}| \quad (47)$$

is the number of codewords in \mathcal{C}_n that have joint type Q with z^n . Therefore, $\{N_Q(z^n) : Q \in \mathcal{P}_n(\mathcal{X} \times \mathcal{Z})\}$ is a multinomial collection with cluster size M and success probabilities

$$p_Q(z^n) = \frac{|\mathcal{T}_Q^n|}{|\mathcal{T}_{Q_Z}^n| |\mathcal{T}_{Q_X}^n|} P_{X^n}(\mathcal{T}_{Q_X}^n) \mathbb{1}\{Q_Z = \hat{Q}_{z^n}\} \quad (48)$$

(where \hat{Q}_{z^n} denotes the type of z^n) for any code sampling distribution $P_{X^n}(x^n)$ that depends on x^n through its type, including our cases of interest. (The above equality is proved in Appendix G.)

Partition $\mathcal{P}_n(\mathcal{X} \times \mathcal{Z}) = \mathcal{Q}'_n \cup \mathcal{Q}''_n$ as

$$\mathcal{Q}'_n \triangleq \{Q \in \mathcal{P}_n(\mathcal{X} \times \mathcal{Z}) : \ell(Q) \leq e^2 M\}, \quad (49)$$

$$\mathcal{Q}''_n \triangleq \{Q \in \mathcal{P}_n(\mathcal{X} \times \mathcal{Z}) : \ell(Q) > e^2 M\}, \quad (50)$$

and, accordingly, split $L(z^n) = L_1(z^n) + L_2(z^n)$ as

$$L_1(z^n) \triangleq \frac{1}{M} \sum_{Q \in \mathcal{Q}'_n} N_Q(z^n) \ell(Q), \quad (51)$$

$$L_2(z^n) \triangleq \frac{1}{M} \sum_{Q \in \mathcal{Q}''_n} N_Q(z^n) \ell(Q). \quad (52)$$

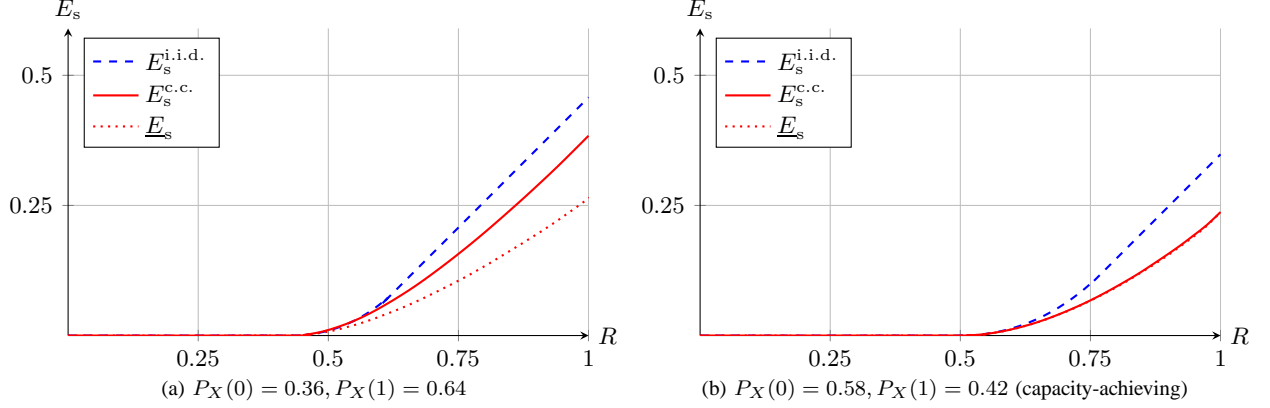


Fig. 4. Comparison of secrecy exponents for Z-channel with $W_E(0|1) = 0.303$

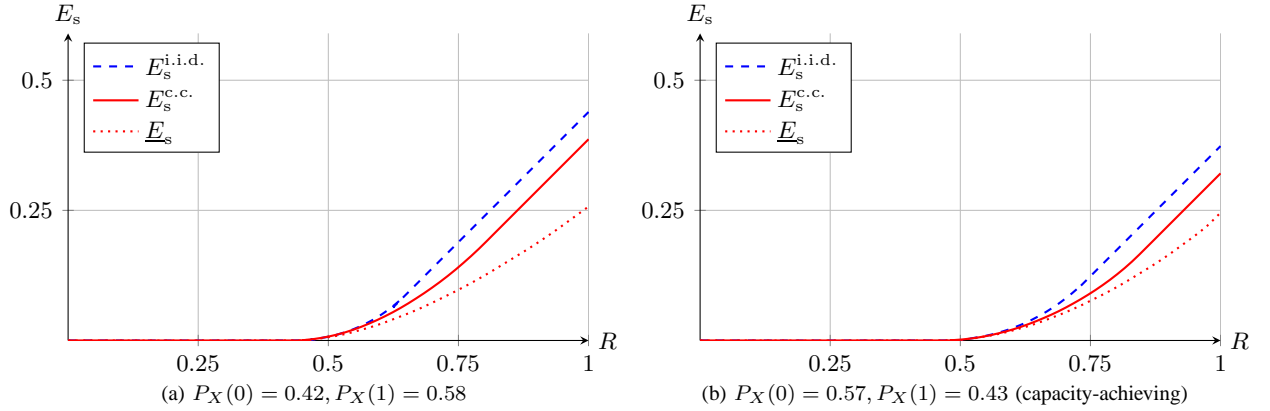


Fig. 5. Comparison of secrecy exponents for binary asymmetric channel with $W_E(1|0) = 0.01$, $W_E(0|1) = 0.303$

Indeed, L_1 turns out to be the light-tail component of L and L_2 its heavy-tail part. Let also,

$$\nu(z^n) \triangleq \text{var}(L_1(z^n)) + \frac{1}{M} \mathbb{E}[L_1(z^n)]^2, \text{ and} \quad (53)$$

$$\mu(z^n) \triangleq \mathbb{E}[L_2(z^n)]. \quad (54)$$

Using elementary properties of multinomial distribution it can be verified that

$$\nu(z^n) = \frac{1}{M} \sum_{Q \in \mathcal{Q}'_n} \ell(Q)^2 p_Q(z^n) \quad (55a)$$

$$\mu(z^n) = \sum_{Q \in \mathcal{Q}''_n} \ell(Q) p_Q(z^n) \quad (55b)$$

(A proof of the above is given in Appendix H for completeness.) In the following two subsections we prove that $\forall z^n \in \text{supp}(\bar{P}_{Z^n})$,

$$\mathbb{E}[L(z^n) \ln L(z^n)] + \frac{1}{M} \doteq \nu(z^n) + \mu(z^n). \quad (56)$$

Since z^n is fixed in both sides of (56) we drop it in subsections V-B and V-C to avoid cumbersome notation.

B. Achievability

For non-negative l_1 and l_2 , and $l = l_1 + l_2$,

$$l \ln(l) = l_1 \ln(l) + l_2 \ln(l) \quad (57)$$

$$= l_1 \ln(l_1) + l_1 \ln(1 + l_2/l_1) + l_2 \ln(l) \quad (58)$$

$$\leq l_1 \ln(l_1) + l_2(1 + \ln(l)) \quad (59)$$

(since $\ln(1 + l_2/l_1) \leq l_2/l_1$), thus,

$$\mathbb{E}[L \ln L] \leq \mathbb{E}[L_1 \ln L_1] + \mathbb{E}[L_2(1 + \ln L)] \quad (60)$$

$$\stackrel{(*)}{\leq} \mathbb{E}[L_1 \ln L_1] + (1 + n \ln \alpha) \mathbb{E}[L_2] \quad (61)$$

where $(*)$ follows from (iii) in Lemma 6 (as $L = L(z^n) \leq 1/\bar{P}_{Z^n}(z^n)$). The upper bound of (41) implies

$$\mathbb{E}[L_1 \ln L_1] \leq \mathbb{E}[L_1] \ln(\mathbb{E}[L_1]) + \frac{\text{var}(L_1)}{\mathbb{E}[L_1]} \stackrel{(*)}{\leq} \frac{\text{var}(L_1)}{\mathbb{E}[L_1]} \quad (62)$$

where $(*)$ follows since $\mathbb{E}[L_1] \leq \mathbb{E}[L] = 1$. Moreover, using (53) and the fact that $\mathbb{E}[L_1] + \mathbb{E}[L_2] = 1$ we have

$$\frac{\text{var}(L_1)}{\mathbb{E}[L_1]} = \frac{\nu}{\mathbb{E}[L_1]} - \frac{\mathbb{E}[L_1]}{M} \quad (63)$$

$$= \nu \left(1 + \frac{\mathbb{E}[L_2]}{\mathbb{E}[L_1]} \right) - \frac{1 - \mathbb{E}[L_2]}{M} \quad (64)$$

$$= \nu + \mathbb{E}[L_2] \left(\frac{\nu}{\mathbb{E}[L_1]} + \frac{1}{M} \right) - \frac{1}{M}. \quad (65)$$

Since $\ell(Q) \leq Me^2$ for $Q \in \mathcal{Q}'_n$, using (55a) we have

$$\nu \leq \frac{1}{M} \sum_{Q \in \mathcal{Q}'_n} e^2 M \cdot \ell(Q) p_Q = e^2 \mathbb{E}[L_1]. \quad (66)$$

Using the above in (65) and replacing $\mathbb{E}[L_2] = \mu$, we get

$$\frac{\text{var}(L_1)}{\mathbb{E}[L_1]} + \frac{1}{M} \leq \nu + \mathbb{E}[L_2] \left(e^2 + \frac{1}{M} \right) \leq \nu + (1 + e^2)\mu, \quad (67)$$

(since $M \geq 1$). Finally, using (67) in (62) yields,

$$\mathbb{E}[L_1 \ln L_1] + \frac{1}{M} \leq \nu + \mu. \quad (68)$$

Using (68) in (61) (and noting that $\alpha \geq 1$ only depends on $|\mathcal{X}|$, P_X , and W) we conclude that

$$\mathbb{E}[L \ln L] + \frac{1}{M} \leq \nu + \mu. \quad (69)$$

C. Ensemble Converse

The choice of \mathcal{Q}''_n implies

$$\Pr\{L_2 \in (0, e^2)\} = 0. \quad (70)$$

This holds since either $\forall Q \in \mathcal{Q}''_n: N_Q = 0$ which implies $L_2 = 0$ or $\exists Q_0 \in \mathcal{Q}''_n$ such that $N_{Q_0} \geq 1$, in which case,

$$L_2 \geq \frac{1}{M} \ell(Q_0) N_{Q_0} \geq \frac{1}{M} \ell(Q_0) \geq e^2, \quad (71)$$

(because $\forall Q \in \mathcal{Q}''_n, \ell(Q) > e^2 M$). Consequently,

$$\mathbb{E}[L_2 \ln L_2] = \sum_{l \geq e^2} l \ln(l) \Pr\{L_2 = l\} \quad (72)$$

$$\geq \ln(e^2) \sum_{l \geq e^2} l \Pr\{L_2 = l\} = 2 \mathbb{E}[L_2]. \quad (73)$$

For positive l_1 and l_2 , and $l = l_1 + l_2 \geq \max\{l_1, l_2\}$,

$$l \ln(l) = l_1 \ln(l) + l_2 \ln(l) \quad (74)$$

$$\geq l_1 \ln(l_1) + l_2 \ln(l_2). \quad (75)$$

Therefore,

$$\mathbb{E}[L \ln L] \geq \mathbb{E}[L_1 \ln L_1] + \mathbb{E}[L_2 \ln L_2]. \quad (76)$$

Using the lower bound of (41) (with $\tau_\theta(L_1)$ and $c(\theta)$ defined as in (42) and (43) respectively), $\forall \theta > 0$:

$$\mathbb{E}[L_1 \ln L_1] \geq \mathbb{E}[L_1] \ln(\mathbb{E}[L_1]) + c(\theta) \left[\frac{\text{var}(L_1)}{\mathbb{E}[L_1]} - \tau_\theta(L_1) \right] \quad (77)$$

$$\stackrel{(a)}{=} (1 - \mathbb{E}[L_2]) \ln(1 - \mathbb{E}[L_2]) + c(\theta) \left[\frac{\text{var}(L_1)}{\mathbb{E}[L_1]} - \tau_\theta(L_1) \right] \quad (78)$$

$$\stackrel{(b)}{\geq} -\mathbb{E}[L_2] + c(\theta) \left[\frac{\text{var}(L_1)}{\mathbb{E}[L_1]} - \tau_\theta(L_1) \right]. \quad (79)$$

In the above (a) follows since $\mathbb{E}[L_1] = 1 - \mathbb{E}[L_2]$ and (b) since $(1 - \varepsilon) \ln(1 - \varepsilon) \geq -\varepsilon$. Using (73) and (79) in (75) shows that $\forall \theta > 0$:

$$\mathbb{E}[L \ln L] \geq c(\theta) \left[\frac{\text{var}(L_1)}{\mathbb{E}[L_1]} - \tau_\theta(L_1) \right] + \mathbb{E}[L_2]. \quad (80)$$

Now we shall upper-bound $\tau_\theta(L_1)$. Starting by bounding the tail of L_1 we have

$$\Pr\{L_1 \geq (v+1) \mathbb{E}[L_1]\} = \Pr\left\{ \sum_{Q \in \mathcal{Q}'_n} \ell(Q) (N_Q - Mp_Q) \geq Mv \mathbb{E}[L_1] \right\} \quad (81)$$

$$\leq \Pr\left\{ \bigcup_{Q \in \mathcal{Q}'_n} \left\{ \ell(Q) (N_Q - Mp_Q) \geq \frac{Mv \mathbb{E}[L_1]}{|\mathcal{Q}'_n|} \right\} \right\} \quad (82)$$

$$\stackrel{(a)}{\leq} \sum_{Q \in \mathcal{Q}'_n} \Pr\left\{ \ell(Q) (N_Q - Mp_Q) \geq \frac{Mv \mathbb{E}[L_1]}{|\mathcal{Q}'_n|} \right\} \quad (83)$$

$$\stackrel{(b)}{\leq} \sum_{Q \in \mathcal{Q}'_n} \frac{\mathbb{E}[\ell(Q)^4 (N_Q - Mp_Q)^4]}{(Mv \mathbb{E}[L_1]/|\mathcal{Q}'_n|)^4} \quad (84)$$

$$= \frac{|\mathcal{Q}'_n|^4}{v^4 (\mathbb{E}[L_1])^4} \frac{1}{M^4} \sum_{Q \in \mathcal{Q}'_n} \ell(Q)^4 \mathbb{E}[(N_Q - Mp_Q)^4], \quad (85)$$

where (a) is the union bound and (b) follows by Markov inequality. For $N \sim \text{Binomial}(M, p)$,

$$\mathbb{E}[(N - Mp)^4] = Mp(1-p)[1 + 3(M-2)p(1-p)] \quad (86)$$

$$\leq \text{var}(N) + 3 \text{var}(N)^2. \quad (87)$$

Continuing (85) we have

$$\frac{1}{M^4} \sum_{Q \in \mathcal{Q}'_n} \ell(Q)^4 \mathbb{E}[(N_Q - Mp_Q)^4] \leq \frac{1}{M^4} \sum_{Q \in \mathcal{Q}'_n} \ell(Q)^4 (\text{var}(N_Q) + 3 \text{var}(N_Q)^2) \quad (88)$$

$$\stackrel{(a)}{\leq} \frac{1}{M^2} \sum_{Q \in \mathcal{Q}'_n} \ell(Q)^2 \text{var}(N_Q) + 3 \frac{1}{M^4} \sum_{Q \in \mathcal{Q}'_n} \ell(Q)^4 \text{var}(N_Q)^2 \quad (89)$$

$$\stackrel{(b)}{\leq} \frac{1}{M^2} \sum_{Q \in \mathcal{Q}'_n} \ell(Q)^2 \text{var}(N_Q) + 3 \left[\frac{1}{M^2} \sum_{Q \in \mathcal{Q}'_n} \ell(Q)^2 \text{var}(N_Q) \right]^2 \quad (90)$$

$$\stackrel{(c)}{\leq} \nu + 3\nu^2 \stackrel{(d)}{=} \nu, \quad (91)$$

where (a) follows since $\ell(Q) \leq e^2 M \doteq M$ for $Q \in \mathcal{Q}'_n$, (b) since for positive summands, the sum of the squares is less than the square of the sums, (c) since $\text{var}(N_Q) \leq Mp_Q$, and (d) since $\nu \leq e^2 \mathbb{E}[L_1] \leq e^2$ (see (66)). Plugging (91) into (85) we get

$$\Pr\{L_1 \geq (v+1) \mathbb{E}[L_1]\} \leq \frac{|\mathcal{Q}'_n|^4 \nu}{(\mathbb{E}[L_1])^4} \cdot \frac{1}{v^4}. \quad (92)$$

Using the above in (42) we get

$$\tau_\theta(L_1) = \mathbb{E}[L_1] \left[\theta^2 \Pr\{L_1 > (\theta+1) \mathbb{E}[L_1]\} + 2 \int_\theta^{+\infty} v \Pr\{L_1 > (v+1) \mathbb{E}[L_1]\} dv \right] \quad (93)$$

$$\leq \mathbb{E}[L_1] \left[\frac{\theta^2}{\theta^4} + 2 \int_\theta^{+\infty} \frac{v}{v^4} dv \right] \frac{|\mathcal{Q}'_n|^4 \nu}{\mathbb{E}[L_1]^4} \quad (94)$$

$$\doteq \frac{\nu}{\mathbb{E}[L_1]^3} \cdot \frac{|\mathcal{Q}'_n|^4}{\theta^2}. \quad (95)$$

Since (95) implies $\tau_\theta(L_1) \leq d(n)|\mathcal{Q}'_n|^4\nu/(\theta^2\mathbb{E}[L_1]^3)$ for some sub-exponentially increasing sequence $d(n)$ (which only depends on $|\mathcal{X}|$ and $|\mathcal{Z}|$), taking

$$\theta_n \triangleq 2\sqrt{d(n)}\frac{|\mathcal{Q}'_n|^2}{\mathbb{E}[L_1]}, \quad (96)$$

we will have

$$\tau_{\theta_n}(L_1) \leq \frac{1}{4} \cdot \frac{\nu}{\mathbb{E}[L_1]}. \quad (97)$$

Using (53) and (97) in (80) we have

$$\mathbb{E}[L(z^n) \ln L(z^n)] \geq c(\theta_n) \left[\frac{\text{var}(L_1)}{\mathbb{E}[L_1]} - \tau_{\theta_n}(L_1) \right] + \mathbb{E}[L_2] \quad (98)$$

$$\geq c(\theta_n) \left[\frac{\nu}{\mathbb{E}[L_1]} - \frac{1}{M} \mathbb{E}[L_1] - \frac{1}{4} \cdot \frac{\nu}{\mathbb{E}[L_1]} \right] + \mathbb{E}[L_2] \quad (99)$$

$$\stackrel{(*)}{\geq} c(\theta_n) \left[\frac{3}{4} \cdot \frac{\nu}{\mathbb{E}[L_1]} - \frac{1}{M} \right] + \mathbb{E}[L_2] \quad (100)$$

(where $(*)$ follows because $\mathbb{E}[L_1] \leq 1$). Since for $\theta > 0$, $c(\theta) \leq c(0) = \frac{1}{2} < 1$, we can further lower-bound (100) as

$$\mathbb{E}[L \ln L] \geq \frac{3}{4}c(\theta_n)\frac{\nu}{\mathbb{E}[L_1]} + \mathbb{E}[L_2] - \frac{1}{M} \quad (101)$$

Moreover,

$$c(\theta_n) = \frac{1}{\theta_n} \cdot \frac{(1+\theta_n)\ln(1+\theta_n) - \theta_n}{\theta_n} \quad (102)$$

$$\stackrel{(a)}{\geq} \frac{1}{\theta_n} \cdot \frac{(1+\mathbb{E}[L_1]\theta_n)\ln(1+\mathbb{E}[L_1]\theta_n) - \mathbb{E}[L_1]\theta_n}{\mathbb{E}[L_1]\theta_n} \quad (103)$$

$$= \mathbb{E}[L_1] \frac{(1+\mathbb{E}[L_1]\theta_n)\ln(1+\mathbb{E}[L_1]\theta_n) - \mathbb{E}[L_1]\theta_n}{(\mathbb{E}[L_1]\theta_n)^2} \quad (104)$$

$$\stackrel{(b)}{\geq} \mathbb{E}[L_1], \quad (105)$$

where (a) follows since $\frac{(1+\theta)\ln(1+\theta)-\theta}{\theta}$ is increasing in θ and $\mathbb{E}[L_1] \leq 1$, and (b) since $\frac{(1+\theta)\ln(1+\theta)-\theta}{\theta^2}$ is decreasing in θ (see Lemma 10 in Appendix F) and $\mathbb{E}[L_1]\theta_n = 2\sqrt{d(n)}|\mathcal{Q}'_n|^2 \leq 2\sqrt{d(n)}(n+1)^{2|\mathcal{X}||\mathcal{Z}|}$. Using this lower bound in (101) we get

$$\mathbb{E}[L \ln L] + \frac{1}{M} \geq \nu + \mu \quad (106)$$

D. Derivation of Exponents for Each Ensemble

Equations (69) and (106) prove (56). Plugging in the values of $\nu(z^n)$ and $\mu(z^n)$ from (55a) and (55b) and continuing (56), we get

$$\mathbb{E}[L(z^n) \ln L(z^n)] + \frac{1}{M} \doteq \nu(z^n) + \mu(z^n) \quad (107)$$

$$= \sum_{Q \in \mathcal{P}_n(\mathcal{X} \times \mathcal{Z})} \ell(Q) p_Q(z^n) \kappa(\ell(Q)/M) \quad (108)$$

where

$$\kappa(\lambda) = \begin{cases} 1 & \lambda > e^2, \\ \lambda & \lambda \leq e^2. \end{cases} \quad (109)$$

It is easy to check that

$$\min\{1, \lambda\} \leq \kappa(\lambda) \leq e^2 \min\{1, \lambda\} \quad (110)$$

Therefore, (108) can be simplified as

$$\begin{aligned} & \mathbb{E}[L(z^n) \ln L(z^n)] + \frac{1}{M} \\ & \doteq \sum_{Q \in \mathcal{P}_n(\mathcal{X} \times \mathcal{Z})} \ell(Q) p_Q(z^n) \min\left\{1, \frac{\ell(Q)}{M}\right\}. \end{aligned} \quad (111)$$

Using the above in (39) we get

$$\begin{aligned} & \mathbb{E}[D(P_{C_n} \| \bar{P}_{Z^n})] + \frac{\log(e)}{M} \\ & \doteq \sum_{z^n \in \mathcal{Z}^n} \bar{P}_{Z^n}(z^n) \sum_{Q \in \mathcal{P}_n(\mathcal{X} \times \mathcal{Z})} \ell(Q) p_Q(z^n) \min\left\{1, \frac{\ell(Q)}{M}\right\} \end{aligned} \quad (112)$$

$$= \sum_{Q \in \mathcal{P}_n(\mathcal{X} \times \mathcal{Z})} \ell(Q) \min\left\{1, \frac{\ell(Q)}{M}\right\} \sum_{z^n \in \mathcal{Z}^n} p_Q(z^n) \bar{P}_{Z^n}(z^n). \quad (113)$$

Plugging in the value of $p_Q(z^n)$ from (48) we get

$$\sum_{z^n \in \mathcal{Z}^n} p_Q(z^n) \bar{P}_{Z^n}(z^n) = \frac{|\mathcal{T}_Q^n|}{|\mathcal{T}_{Q_X}^n| |\mathcal{T}_{Q_Z}^n|} P_{X^n}(\mathcal{T}_{Q_X}^n) \bar{P}_{Z^n}(\mathcal{T}_{Q_Z}^n). \quad (114)$$

Moreover, defining

$$\omega(Q) = \sum_{x,z} Q(x,z) \log W(z|x), \quad (115)$$

and recalling that \bar{P}_{Z^n} depends on z^n only through its type, we deduce that

$$\ell(Q) = \frac{\exp(n\omega(Q))}{\bar{P}_{Z^n}(\mathcal{T}_{Q_Z}^n)/|\mathcal{T}_{Q_Z}^n|} \quad (116)$$

Combining (114) and (116) yields

$$\ell(Q) \sum_{z^n} p_Q(z^n) \bar{P}_{Z^n}(z^n) = \exp\{n\omega(Q)\} |\mathcal{T}_Q^n| \frac{P_{X^n}(\mathcal{T}_{Q_X}^n)}{|\mathcal{T}_{Q_X}^n|} \quad (117)$$

$$\doteq \exp\{-nD(Q \| Q_X \times W)\} P_{X^n}(\mathcal{T}_{Q_X}^n), \quad (118)$$

where the last equality follows since $|\mathcal{T}_Q^n| \doteq \exp\{nH(Q)\}$ (respectively, $|\mathcal{T}_{Q_X}^n| \doteq \exp\{nH(Q_X)\}$). Thus, we have

$$\begin{aligned} & \mathbb{E}[D(P_{C_n} \| \bar{P}_{Z^n})] + \frac{\log(e)}{M} \\ & \doteq \sum_{Q \in \mathcal{P}_n(\mathcal{X} \times \mathcal{Z})} \exp\{-nD(Q \| Q_X \times W)\} \\ & \quad \times P_{X^n}(\mathcal{T}_{Q_X}^n) \min\left\{1, \frac{\ell(Q)}{M}\right\}. \end{aligned} \quad (119)$$

Observe that since

$$\ell(P_{XZ}) \geq \exp\{n\omega(P_{XZ})\} |\mathcal{T}_{P_Z}^n| \geq \exp\{nI(X;Z)\}, \quad (120)$$

taking $Q = P_{XZ}$ shows that the right-hand-side of (119) decays at most as fast as $\exp\{-n[R - I(X;Z)]^+\}$ which is strictly slower than $\frac{1}{M} = \exp(-nR)$ since $I(X;Z) > 0$.

Consequently we can ignore the term $\frac{\log(e)}{M}$ on the left-hand-side of (119) and conclude that

$$\mathbb{E}[D(P_{C_n} \|\bar{P}_{Z^n})] \doteq \sum_{Q \in \mathcal{P}_n(\mathcal{X} \times \mathcal{Z})} \exp\{-nD(Q \| Q_X \times W)\} \\ \times P_{X^n}(\mathcal{T}_{Q_X}^n) \min\left\{1, \frac{\ell(Q)}{M}\right\}. \quad (121)$$

(The careful reader may argue that P_{XZ} may not be an n -type for all n and, hence, find our reasoning for the passage from (119) to (121) inaccurate. While this concern is valid, the claim is true regardless as we can always find a sequence of n -types that converge to P_{XZ} . We give a rigorous and more detailed proof of (121) in Appendix I.)

1) *Ensemble of i.i.d. random codes:* When $P_{X^n} = P_X^n$,

$$P_{X^n}(\mathcal{T}_{Q_X}^n) \doteq \exp\{-nD(Q_X \| P_X)\} \quad (122)$$

Moreover, $\bar{P}_{Z^n}(z^n) = P_Z^n(z^n)$ (where $P_Z = P_X \circ W$). Therefore, $\bar{P}_{Z^n}(z^n) = \exp\{n \sum_z Q_Z(z) \log P_Z(z)\}$ if $z^n \in \mathcal{T}_{Q_Z}^n$. Therefore,

$$\ell(Q) = \frac{\exp\{n\omega(Q)\}}{P_Z^n(z^n)} = \exp\left\{n \sum_{x,z} Q(x,z) \log \frac{W(z|x)}{P_Z(z)}\right\} \\ = \exp\{nf(Q \| P_{XZ})\}. \quad (123)$$

where f is defined in (25b). As a consequence,

$$\min\{1, \ell(Q)/M\} \doteq \exp\{-n[R - f(Q \| P_{XZ})]^+\}. \quad (124)$$

Using (122) and (124) in (121) (together with the fact that $|\mathcal{P}_n(\mathcal{X} \times \mathcal{Z})| \leq (n+1)^{|\mathcal{X}||\mathcal{Z}|}$) conclude that

$$\mathbb{E}[D(P_{C_n} \|\bar{P}_{Z^n})] \doteq \exp\left\{-n \min_{Q \in \mathcal{P}_n(\mathcal{X} \times \mathcal{Z})} \left\{D(Q \| Q_X \times W) \right. \right. \\ \left. \left. + D(Q_X \| P_X) + [R - f(Q \| P_{XZ})]^+\right\}\right\}. \quad (125)$$

Simplifying the above exponent yields (25).

2) *Ensemble of constant-composition random codes:* When the code sampling distribution, P_{X^n} , is the uniform distribution over the type-class $\mathcal{T}_{P_n}^n$, $P_{X^n}(\mathcal{T}_{Q_X}^n) = 0$ unless $Q_X = P_n$, i.e., $Q = P_n \times V$ for some $V: \mathcal{X} \rightarrow \mathcal{Z}$ such that $P_n \times V \in \mathcal{P}_n(\mathcal{X} \times \mathcal{Z})$. (To keep the notation simple, we omit this last condition from the following equations.) Therefore (121) reduces to

$$\mathbb{E}[D(P_{C_n} \|\bar{P}_{Z^n})] \doteq \sum_{V: \mathcal{X} \rightarrow \mathcal{Z}} \exp\{-nD(V \| W | P_n)\} \\ \times \min\{1, \ell(P_n \times V)/M\}. \quad (126)$$

It remains to evaluate

$$\ell(P_n \times V) = \frac{W^n(z^n | x^n)}{\bar{P}_{Z^n}(z^n)}, \quad (127)$$

for some $x^n \in \mathcal{T}_{P_n}^n$ and $z^n \in \mathcal{T}_V^n(x^n)$, where $\mathcal{T}_V^n(x^n)$ is the V -shell of x^n . To this end, we note that

$$\bar{P}_{Z^n}(z^n) = \frac{1}{|\mathcal{T}_{P_n}^n|} \sum_{x^n \in \mathcal{T}_{P_n}^n} W(z^n | x^n) \quad (128)$$

$$= \frac{1}{|\mathcal{T}_{P_n}^n|} \sum_{x^n \in \mathcal{T}_{P_n}^n} W(z^n | x^n) \sum_{V': \mathcal{X} \rightarrow \mathcal{Z}} \mathbb{1}\{z^n \in \mathcal{T}_{V'}^n(x^n)\} \quad (129)$$

$$= \frac{1}{|\mathcal{T}_{P_n}^n|} \sum_{x^n \in \mathcal{T}_{P_n}^n} \sum_{V': \mathcal{X} \rightarrow \mathcal{Z}} \mathbb{1}\{z^n \in \mathcal{T}_{V'}^n(x^n)\} W(z^n | x^n) \quad (130)$$

$$= \frac{1}{|\mathcal{T}_{P_n}^n|} \sum_{x^n \in \mathcal{T}_{P_n}^n} \sum_{V': \mathcal{X} \rightarrow \mathcal{Z}} \mathbb{1}\{z^n \in \mathcal{T}_{V'}^n(x^n)\} \\ \times \exp[-n(D(V' \| W | P_n) + H(V' | P_n))] \quad (131)$$

$$= \sum_{V': \mathcal{X} \rightarrow \mathcal{Z}} \frac{1}{|\mathcal{T}_{P_n}^n|} \sum_{x^n \in \mathcal{T}_{P_n}^n} \mathbb{1}\{z^n \in \mathcal{T}_{V'}^n(x^n)\} \\ \times \exp[-n(D(V' \| W | P_n) + H(V' | P_n))]. \quad (132)$$

(Recall again that V' must also be such that $P_n \times V'$ is an n -type but we omit this condition from the equations for the sake of brevity.) As we have already shown in the proof of (48) (cf. Appendix G),

$$\frac{1}{|\mathcal{T}_{P_n}^n|} \sum_{x^n \in \mathcal{T}_{P_n}^n} \mathbb{1}\{z^n \in \mathcal{T}_{V'}^n(x^n)\} \\ = \frac{|\mathcal{T}_{P_n \times V'}^n|}{|\mathcal{T}_{P_n}^n| |\mathcal{T}_{P_n \circ V'}^n|} \mathbb{1}\{P_n \circ V' = \hat{Q}_{z^n}\} \quad (133) \\ \doteq \exp[n(H(V' | P_n) - H(P_n \circ V'))] \mathbb{1}\{P_n \circ V' = \hat{Q}_{z^n}\} \quad (134)$$

(where \hat{Q}_{z^n} is the type of z^n). Using (134) in (132) and recalling that z^n has type $P_n \circ V$ we get

$$\bar{P}_{Z^n}(z^n) \doteq \exp\left[-n[H(P_n \circ V) \right. \\ \left. + \min_{\substack{V': \mathcal{X} \rightarrow \mathcal{Z} \\ P_n \circ V' = P_n \circ V}} D(V' \| W | P_n)]\right], \quad (135)$$

which, in turn, shows

$$\ell(P_n \times V) \doteq \exp[-ng_n(V \| W | P_n)] \quad (136)$$

with g_n defined as in (27b). Therefore,

$$\min\{1, \ell(P_n \times V)/M\} \doteq \exp[-n[R - g_n(V \| W | P_n)]^+]. \quad (137)$$

Using (137) in (126) proves (27). ■

VI. CONCLUSION AND DISCUSSION

We studied the *exact* exponential decay rate of the information leaked to the eavesdropper in Wyner's wiretap channel setting when an average wiretap channel code in the ensemble of i.i.d. or constant-composition random codes is used for communication. Our analysis shows that the previously-derived lower bound on the secrecy exponent of i.i.d. random codes in [8]–[11] is, indeed, tight. Moreover, our result for

constant-composition random codes improves upon that of [13] (see (34) and examples in Section IV-B).

A key step in our analysis (which is applicable to any ensemble of random codes with independently sampled code-words) is to observe the equivalence of secrecy and resolvability exponents for the ensemble and, as a result, reducing the problem to the analysis of the resolvability exponent. The latter is easier as the informational divergence of interest (whose exponential decay rate is being assessed) involves a single random distribution (the output distribution) while the former involves two (the conditional and unconditional output distributions). We should emphasize that establishing secrecy via channel resolvability is a standard technique which was used in [5], [7], [10], [11], [15] (also, in combination with privacy amplification in [8], [13]) whose advantages are discussed in [4]. Our result (Theorem 1) highlights the usefulness of this tool by showing that the resolvability exponent is not only a lower bound to the secrecy exponent but also equals the secrecy exponent.

Thanks to such a reduction, we extended the method of [11] to derive the exact resolvability exponent of random codes. It is noteworthy that, as it was already envisioned in [11], the method presented there was conveniently applicable to the ensemble of constant-composition random codes (as well as the ensemble of i.i.d. random codes already studied in [11]).

It is remarkable that, unlike the channel coding problem for which constant-composition random codes turn out to be never worse than i.i.d. random codes in terms of the exponent [22], for the secrecy problem we have examples (see Figures 4 and 5) where i.i.d. random codes perform better than constant-composition codes. The examples presented in Section IV-B suggest that the superior ensemble (in terms of the secrecy exponent) depends on the channel W_E alone (i.e., for a given channel, either of the ensembles yields a better secrecy exponent for all input distributions). A subject for future research would be to characterize the set of channels for which the ensemble of i.i.d. random codes results in a better secrecy exponent (and vice versa).

As shown in [2], for general pairs of channels (W_M, W_E) , the secrecy capacity is given by

$$\max_{\substack{P_{UX}: \\ U \leftrightarrow X \leftrightarrow (Y, Z)}} \{I(U; Y) - I(U; Z)\}. \quad (138)$$

The secrecy capacity equals

$$\max_{P_X} \{I(X; Y) - I(X; Z)\} \quad (139)$$

when $\forall P_X, I(X; Y) \geq I(X; Z)$. Accordingly, for the general case and when the secrecy capacity is positive, one can construct wiretap channel codes by prefixing the channel with an auxiliary channel $P_{X|U} : \mathcal{U} \rightarrow \mathcal{X}$. Channel prefixing is also proposed in [10] as a technique to treat the wiretap channels with cost constraints. (The auxiliary channel $P_{X|U}$ will be chosen such that its output sequence satisfies the cost constraints for the physical channel.) It is obvious that our results (as well as those of others cited) are immediately extensible to such cases. More precisely, for a given auxiliary channel $P_{X|U}$, the exponents of (29) and (31), evaluated for the effective channel

$P_{Z|U}(z|u) = \sum_x P_{X|U}(x|u) W_E(z|x)$ (instead of W_E) and the input distribution P_U are the ensemble-optimal secrecy exponents of both random-coding ensembles. Observe that in this setting $P_{X|U}$ (in addition to the random-binning rate R) is also a design parameter which can be exploited to optimize the secrecy exponent.³ Moreover, it should also be noted that in the prefixed setting, in addition to the entropy rate of R bits per channel use (for random binning), the encoder requires an entropy rate of $H(X|U)$ bits per channel use to simulate the channel $P_{X|U}$ that has to be taken into account in comparison of the secrecy exponents.

APPENDIX A PROOF OF THEOREM 2

Consider the sequence of random wiretap channel codes of secret message size $2M_s$, $M_s = \exp(nR_s)$ and random binning rate R in the sense of Definition 8. Namely, those obtained by partitioning a random code of size $2\exp[n(R + R_s)]$ into $2M_s$ sub-codes of rate R . (Assume R and R_s are chosen such $\exp[n(R + R_s)]$, $\exp(nR_s)$ and $\exp(nR)$ are all integers for notational brevity.) Let

$$\bar{P}_{e,n} \triangleq \mathbb{E}[\Pr\{\hat{s}_{ML}(Y^n) \neq S\}], \quad (140)$$

$$\bar{D}_n \triangleq \mathbb{E}[D(P_{C_n^S} \| \bar{P}_{Z^n} | P_S)]. \quad (141)$$

when S is uniformly distributed on $\{1, 2, \dots, 2M_s\}$ with Y^n and Z^n being the output sequences of the legitimate receiver's and wiretapper's channel respectively as in Figure 1, $P_{C_n^S}$ being the distribution of wiretapper's channel output sequence when a uniformly chosen codeword from the sub-code C_n^S is transmitted (see (8)) and \bar{P}_{Z^n} the distribution induced by codeword sampling distribution at the output of wiretapper's channel (see (12)). (The expectation is taken over the choice of codebook $\mathcal{C}_n = \bigcup_{s=1}^{2M_s} C_n^s$). By the assumptions of Theorem (in particular, the continuity of E_r in rate) and the linearity of expectation we have

$$\liminf_{n \rightarrow \infty} -\frac{1}{n} \log(\bar{P}_{e,n}) \geq \underline{E}_r(\Pi, W_M, R_s + R), \quad (142)$$

$$\liminf_{n \rightarrow \infty} -\frac{1}{n} \log(\bar{D}_n) \geq \underline{E}_r(\Pi, W_E, R). \quad (143)$$

Markov's inequality implies that for each n , with probability at least $\frac{2}{3}$ over the choice of random codes

$$\Pr\{\hat{s}_{ML}(Y^n) \neq S\} = \frac{1}{2M_s} \sum_{s=1}^{2M_s} \Pr\{\hat{s}_{ML}(Y^n) \neq S | S = s\} \leq 3\bar{P}_{e,n}, \quad (144)$$

and, with probability at least $\frac{2}{3}$

$$D(P_{C_n^S} \| \bar{P}_{Z^n} | P_S) = \frac{1}{2M_s} \sum_{s=1}^{2M_s} D(P_{C_n^s} \| \bar{P}_{Z^n}) \leq 3\bar{D}_n. \quad (145)$$

Therefore, with probability at least $\frac{1}{3}$, the random code is chosen such that both bounds of (144) and (145) simultaneously hold. Let C_n^s , $s \in \{1, 2, \dots, 2M_s\}$ be the collection of sub-codes that define any such good code. Since the summands in

³The authors thank the anonymous reviewer for bringing this point to their attention.

the summation of (144) are all positive, there exists a subset $\mathcal{S}_{n,e} \subseteq \{1, 2, \dots, 2M_s\}$ of cardinality $|\mathcal{S}_{n,e}| > \frac{3}{2}M_s$ such that $\forall s \in \mathcal{S}_{n,e}$,

$$\Pr\{\hat{s}_{\text{ML}}(Y^n) \neq S | S = s\} \leq 12\bar{P}_{e,n}. \quad (146)$$

Similarly, since the summands in (145) are positive, there exists a subset $\mathcal{S}_{n,s} \subseteq \{1, 2, \dots, 2M_s\}$ of cardinality $|\mathcal{S}_{n,s}| > \frac{3}{2}M_s$ such that $\forall s \in \mathcal{S}_{n,s}$

$$D(P_{C^s} \| \bar{P}_{Z^n}) \leq 12\bar{D}_n. \quad (147)$$

Pick any $\mathcal{S}_n \subseteq \mathcal{S}_{n,e} \cap \mathcal{S}_{n,s}$ of cardinality $|\mathcal{S}_n| = M_s$ (this is possible since $|\mathcal{S}_{n,e} \cap \mathcal{S}_{n,s}| \geq M_s$) and consider the wiretap channel code that associates the sub-code C_n^s to each message $s \in \mathcal{S}_n$. This is a code of secret message rate R_s and, when it is employed with any prior P_S on secret messages, satisfies

$$\Pr\{\hat{s}_{\text{ML}}(Y^n) \neq S\} \leq 12\bar{P}_{e,n}, \quad (148)$$

due to (146), and

$$I(S; Z^n) \leq D(P_{C_n^s} \| \bar{P}_{Z^n} | P_S) \leq 12\bar{D}_n, \quad (149)$$

due to (147). Using this sequence of expurgated codes we will have

$$\begin{aligned} \liminf_{n \rightarrow \infty} -\frac{1}{n} \log \Pr\{\hat{s}_{\text{ML}}(Y^n) \neq S\} &\geq \liminf_{n \rightarrow \infty} -\frac{1}{n} \bar{P}_{e,n} \\ &\geq \underline{E}_r(\Pi, W_M, R + R_s) \end{aligned} \quad (150)$$

by combining (148) and (142), and

$$\liminf_{n \rightarrow \infty} -\frac{1}{n} \log I(S; Z^n) \geq \liminf_{n \rightarrow \infty} -\frac{1}{n} \bar{D}_n \geq \underline{E}_s(\Pi, W_E, R) \quad (151)$$

by combining (149) and (143), respectively. ■

Remark. The secrecy part of the proof hinges on finding $\exp(nR_s)$ “good” resolvability codes via expurgation: we first generated twice as many resolvability codes as we needed and then threw away the “bad” half. Very recently, in [31], it was shown that the probability of choosing a bad resolvability code, namely a code C_n (of block-length n) for which the ℓ_1 distance between the output distribution P_{C_n} (8) and the reference measure \bar{P}_{Z^n} is more than $\exp(-n\gamma)$ for some exponent γ , is *doubly exponentially small in n* . This suggests that even if we draw $\exp(nR_s)$ codes in a single-shot from the ensemble, with very high probability they are *all* good resolvability codes. Nevertheless, we do not know if the results of [31] hold for the exponents presented in this work. (Also in this work we measure the approximation quality by KL divergence as opposed to ℓ_1 norm but, at least for the i.i.d. random coding ensemble the KL divergence has the same exponential decay rate as the ℓ_1 distance [25, Equation (30)].)

APPENDIX B PROOF OF THEOREM 4

The results when $I(P_X, W) = 0$ are trivial. So we only proceed with the proofs for the case $I(P_X, W) > 0$.

A. Proof of (i)

Let $P_{XZ} = P_X \times W$ for the sake of brevity. We need to show that

$$\lim_{n \rightarrow \infty} E_{s,n}^{\text{i.i.d.}}(P_X, W, R) = E_s^{\text{i.i.d.}}(P_X, W, R). \quad (152)$$

Recall that $E_{s,n}^{\text{i.i.d.}}$ and $E_s^{\text{i.i.d.}}$ are defined in (25) and (29) respectively. Since $\mathcal{P}_n(\mathcal{X} \times \mathcal{Z}) \subset \mathcal{P}(\mathcal{X} \times \mathcal{Z})$ we trivially have

$$\lim_{n \rightarrow \infty} E_{s,n}^{\text{i.i.d.}}(P_X, W, R) \geq E_s^{\text{i.i.d.}}(P_X, W, R) \quad (153)$$

Let Q^* be the minimizing distribution in the right-hand-side of (29). Since $\bigcup_{n \in \mathbb{N}} \mathcal{P}_n(\mathcal{X} \times \mathcal{Z})$ is dense in $\mathcal{P}(\mathcal{X} \times \mathcal{Z})$, there exists a sequence of n -types $\{Q_n^* \in \mathcal{P}_n(\mathcal{X} \times \mathcal{Z})\}_{n \in \mathbb{N}}$ such that $\lim_{n \rightarrow \infty} |Q_n^* - Q^*| = 0$. We, also have,

$$D(Q_n^* \| P_{XZ}) + [R - f(Q_n^* \| P_{XZ})]^+ \geq E_{s,n}^{\text{i.i.d.}}(P_X, W, R) \quad (154)$$

Moreover we note that $Q^* \ll P_{XZ}$ (for if it is not $D(Q^* \| P_{XZ}) = +\infty$ and Q^* cannot be the minimizer). Consequently, we can assume $\forall n \in \mathbb{N}$, $Q_n^* \ll P_{XZ}$. Since both $D(Q \| P_{XZ})$ and $f(Q \| P_{XZ})$ are continuous in Q over the set of distributions Q that are absolutely continuous with respect to P_{XZ} ,

$$\begin{aligned} \lim_{n \rightarrow \infty} D(Q_n^* \| P_{XZ}) + [R - f(Q_n^* \| P_{XZ})]^+ \\ = D(Q^* \| P_{XZ}) + [R - f(Q^* \| P_{XZ})]^+ \end{aligned} \quad (155)$$

$$= E_s^{\text{i.i.d.}}(P_X, W, R). \quad (156)$$

Using (154) in the above yields,

$$E_s^{\text{i.i.d.}}(P_X, W, R) \geq \lim_{n \rightarrow \infty} E_{s,n}^{\text{i.i.d.}}(P_X, W, R) \quad (157)$$

which, together with (153) prove (152).

B. Proof of (ii)

1) *Preliminaries:* Let us first examine some properties of the functions g and g_n defined in (31b) and (27b) respectively. To this end, it is more convenient to look at g and g_n as mappings from the joint distribution $Q = P \times V \in \mathcal{P}(\mathcal{X} \times \mathcal{Z})$ to \mathbb{R} , namely,

$$\begin{aligned} g(Q, W) &\triangleq \sum_{x,z} Q(x, z) \log W(z|x) + H(Q_Z) \\ &\quad + \min_{\substack{Q' \in \mathcal{P}(\mathcal{X} \times \mathcal{Z}): \\ Q'_X = Q_X, \\ Q'_Z = Q_Z}} D(Q' \| Q'_X \times W), \end{aligned} \quad (158)$$

$$\begin{aligned} g_n(Q, W) &\triangleq \sum_{x,z} Q(x, z) \log W(z|x) + H(Q_Z) \\ &\quad + \min_{\substack{Q' \in \mathcal{P}_n(\mathcal{X} \times \mathcal{Z}): \\ Q'_X = Q_X, Q'_Z = Q_Z}} D(Q' \| Q'_X \times W), \end{aligned} \quad (159)$$

Let us also define the sets $\mathcal{Q} \subseteq \mathcal{P}(\mathcal{X} \times \mathcal{Z})$ and $\mathcal{Q}_n \subseteq \mathcal{P}_n(\mathcal{X} \times \mathcal{Z})$ as

$$\mathcal{Q} \triangleq \{Q \in \mathcal{P}(\mathcal{X} \times \mathcal{Z}): Q \ll Q_X \times W\}. \quad (160)$$

$$\mathcal{Q}_n \triangleq \{Q \in \mathcal{P}_n(\mathcal{X} \times \mathcal{Z}): Q \ll Q_X \times W\}. \quad (161)$$

(Note that $\mathcal{Q}_n = \mathcal{P}_n(\mathcal{X} \times \mathcal{Z}) \cap \mathcal{Q}$.) The set \mathcal{Q} is compact and convex.

Lemma 8. *The function $g(Q, W)$ defined in (158) is continuous in Q over the set of distributions $Q \in \mathcal{Q}$.*

Proof: The linear part $\sum_{x,z} Q(x, z) \log W(z|x)$ is continuous in Q as long as $Q(x, z) = 0$ whenever $W(z|x) = 0$ (which is the case for $Q \in \mathcal{Q}$). The entropy $H(Q_Z)$ is also continuous. It remains to prove the continuity of the last minimization. We first note that

$$\min_{\substack{Q' \in \mathcal{P}(\mathcal{X} \times \mathcal{Z}): \\ Q'_X = Q_X, \\ Q'_Z = Q_Z}} D(Q' \| Q'_X \times W) = \min_{\substack{Q' \in \mathcal{Q}: \\ Q'_X = Q_X, \\ Q'_Z = Q_Z}} D(Q' \| Q'_X \times W) \quad (162)$$

(for if $Q' \notin \mathcal{Q}$, $D(Q' \| Q'_X \times W) = +\infty$ while $Q' = Q$ is a feasible point for the minimization where the objective functions has a finite value). The minimum in the above is well-defined as \mathcal{Q} is compact. Let

$$\phi(Q) \triangleq \min_{\substack{Q' \in \mathcal{Q}: \\ Q'_X = Q_X, Q'_Z = Q_Z}} D(Q' \| Q'_X \times W). \quad (163)$$

We prove that $\phi(Q)$ is convex in Q : Take two distributions Q_1 and Q_2 in \mathcal{Q} and let $Q = \lambda Q_1 + \bar{\lambda} Q_2$ for some $\lambda \in [0, 1]$ (where we use the short-hand notation of $\bar{\lambda} = 1 - \lambda$). Let

$$Q_j^* \triangleq \arg \min_{\substack{Q' \in \mathcal{Q}: \\ Q'_X = (Q_j)_X, Q'_Z = (Q_j)_Z}} D(Q' \| Q'_X \times W), \quad j = 1, 2, \quad (164)$$

be the minimizers of (163). We, hence, have

$$\lambda \phi(Q_1) + \bar{\lambda} \phi(Q_2) = \lambda D(Q_1^* \| (Q_1^*)_X \times W) + \bar{\lambda} D(Q_2^* \| (Q_2^*)_X \times W) \quad (165)$$

$$\stackrel{(a)}{\geq} D(\lambda Q_1^* + \bar{\lambda} Q_2^* \| \lambda (Q_1^*)_X \times W + \bar{\lambda} (Q_2^*)_X \times W) \quad (166)$$

$$\stackrel{(b)}{\geq} \min_{\substack{Q' \in \mathcal{Q}: \\ Q'_X = Q_X, Q'_Z = Q_Z}} D(Q' \| Q'_X \times W) = \phi(Q). \quad (167)$$

where (a) follows since KL divergence is convex in both arguments [22, Lemma 3.5], and (b) follows since the joint distribution $\lambda Q_1^* + \bar{\lambda} Q_2^*$ has x -marginal equal to Q_X and z -marginal equal to Q_Z . The convexity of ϕ implies its continuity in the interior of the set \mathcal{Q} . The only discontinuity points of ϕ could be at the boundaries of the set \mathcal{Q} where it may jump up. We prove that this cannot happen.

Let $\{Q_n \in \mathcal{Q}\}_{n \in \mathbb{N}}$ be a sequence of distributions and $Q = \lim_{n \rightarrow \infty} Q_n$ be its limit point in \mathcal{Q} . Let

$$Q_n^* \triangleq \arg \min_{\substack{Q' \in \mathcal{Q}: \\ Q'_X = (Q_n)_X, Q'_Z = (Q_n)_Z}} D(Q' \| Q'_X \times W) \quad (168)$$

and $Q^* = \lim_{n \rightarrow \infty} Q_n^*$ (by passing to a subsequence if necessary). Since $D(Q \| Q_X \times W)$ is continuous in Q when $Q \ll Q_X \times W$,

$$\lim_{n \rightarrow \infty} \phi(Q_n) = D(Q^* \| Q_X^* \times W). \quad (169)$$

Moreover, since $(Q_n^*)_X = (Q_n)_X$, by continuity of projection we have $Q_X^* = \lim_{n \rightarrow \infty} (Q_n^*)_X = \lim_{n \rightarrow \infty} (Q_n)_X = Q_X$. Similarly, $Q_Z^* = Q_Z$. Thus,

$$\begin{aligned} \lim_{n \rightarrow \infty} \phi(Q_n) &= D(Q^* \| Q_X^* \times W) \\ &\geq \min_{\substack{Q' \in \mathcal{Q}: \\ Q'_X = Q_X, \\ Q'_Z = Q_Z}} D(Q' \| Q'_X \times W) = \phi(Q), \end{aligned} \quad (170)$$

which shows $\phi(Q)$ cannot jump up, hence, $\forall Q \in \mathcal{Q}$, is continuous. ■

Remark. It can be checked that for a fixed P and W , the function $g(V \| W | P)$, defined in (31b), is convex in V .

Lemma 9. *Let $\{Q_n \in \mathcal{Q}_n\}_{n \in \mathbb{N}}$ be a sequence of n -types and $Q = \lim_{n \rightarrow \infty} Q_n \in \mathcal{Q}$ its limit point (note that since $Q_n \in \mathcal{Q}$ and \mathcal{Q} is compact, by passing to a subsequence if necessary, the limit exists). Then,*

$$\lim_{n \rightarrow \infty} g_n(Q_n, W) = g(Q, W) \quad (171)$$

(where $g_n(Q_n, W)$ and $g(Q, W)$ are defined in (158) and (159) respectively).

Proof: Same considerations as in the proof of Lemma 8 shows that when $Q \in \mathcal{Q}_n$, the minimizing Q' on the right-hand-side of (159) must be in \mathcal{Q}_n . Define (for $Q \in \mathcal{Q}_n$),

$$\phi_n(Q) \triangleq \min_{\substack{Q' \in \mathcal{Q}_n: \\ Q'_X = Q_X, Q'_Z = Q_Z}} D(Q' \| Q'_X \times W). \quad (172)$$

Since the linear term $\sum_{x,z} Q(x, z) \log W(z|x)$ (for $Q \in \mathcal{Q}$) and entropy $H(Q_Z)$ are continuous, it is sufficient to prove

$$\lim_{n \rightarrow \infty} \phi_n(Q_n) = \phi(Q) \quad (173)$$

where $\phi(Q)$ is defined in (163). Since $\mathcal{Q}_n \subset \mathcal{Q}$, we trivially have $\phi_n(Q_n) \geq \phi(Q_n)$ and since ϕ is continuous (as shown in Lemma 8), we have

$$\lim_{n \rightarrow \infty} \phi_n(Q_n) \geq \phi(Q). \quad (174)$$

To prove the reverse inequality, let

$$Q^* \triangleq \arg \min_{\substack{Q' \in \mathcal{Q}: \\ Q'_X = Q_X, Q'_Z = Q_Z}} D(Q' \| Q'_X \times W). \quad (175)$$

Since the union of n -types is dense in the simplex, there exists a sequence of n -types $\{Q_n^*\}_{n \in \mathbb{N}}$ such that $\forall n \in \mathbb{N}$, $Q_n^* \ll Q^*$ and $\lim_{n \rightarrow \infty} |Q_n^* - Q^*| = 0$, therefore $\phi(Q) = \lim_{n \rightarrow \infty} D(Q_n^* \| (Q_n^*)_X \times W)$. Moreover, it is easy to verify that $\forall n$, $Q_n^* \in \mathcal{Q}_n$. Unfortunately, the x - and z -marginals of Q_n^* are not necessarily equal to $(Q_n)_X$ and $(Q_n)_Z$ respectively. Therefore we cannot immediately lower-bound $D(Q_n^* \| (Q_n^*)_X \times W)$ by $\phi_n(Q_n)$ to conclude the proof. However, since the marginals of Q_n^* are close to $(Q_n)_X$ and $(Q_n)_Z$, by perturbing Q_n^* s we can find a second sequence of n -types, $\{Q_n^{**}\}_{n \in \mathbb{N}}$ such that

- (a) $(Q_n^{**})_X = (Q_n)_X$ and $(Q_n^{**})_Z = (Q_n)_Z$;
- (b) $Q_n^{**} \in \mathcal{Q}_n$; and
- (c) $\lim_{n \rightarrow \infty} |Q_n^{**} - Q_n^*| = 0$.

Accepting the existence of such a sequence $\{Q_n^{**}\}_{n \in \mathbb{N}}$ we will have

$$\phi(Q) = \lim_{n \rightarrow \infty} D(Q_n^{**} \| (Q_n^*)_X \times W) \quad (176)$$

$$= \lim_{n \rightarrow \infty} D(Q_n^{**} \| (Q_n^*)_X \times W) \quad (177)$$

$$\geq \lim_{n \rightarrow \infty} \phi_n(Q_n) \quad (178)$$

(where the last inequality follows since $D(Q_n^{**} \| (Q_n^*)_X \times W) \geq \phi_n(Q_n)$ as the x - and z -marginals of Q_n^{**} are equal to $(Q_n)_X$ and $(Q_n)_Z$ respectively). This will conclude the proof.

It remains to show the existence of the sequence $\{Q_n^{**}\}_{n \in \mathbb{N}}$. More precisely, we shall show that $\forall \epsilon > 0, \exists n_0(\epsilon)$ such $\forall n > n_0$, we can find $\delta(x, z) : \mathcal{X} \times \mathcal{Z} \rightarrow \mathbb{R}$ with the following properties:

- 1) $n\delta(x, z) \in \mathbb{Z}$;
- 2) with

$$\delta_X(x) \triangleq (Q_n)_X(x) - (Q_n^*)_X(x), \quad \text{and} \quad (179)$$

$$\delta_Z(z) \triangleq (Q_n)_Z(z) - (Q_n^*)_Z(z), \quad (180)$$

we have $\forall x \in \mathcal{X}, \sum_{z \in \mathcal{Z}} \delta(x, z) = \delta_X(x)$, and $\forall z \in \mathcal{Z}, \sum_{x \in \mathcal{X}} \delta(x, z) = \delta_Z(z)$.

- 3) $\forall (x, z) \in \mathcal{X} \times \mathcal{Z}, \delta(x, z) + Q_n^*(x, z) \geq 0$ with equality if $Q_n^*(x, z) = 0$;
- 4) $|\delta| \triangleq \sum_{x, z} |\delta(x, z)| \leq \epsilon$.

(Note that $\delta(x, z)$ also depends on n but we do not show this dependence explicitly to keep the notation simple.) If such δ can be found, $Q_n^{**}(x, z) \triangleq Q_n^*(x, z) + \delta(x, z)$ will be an n -type (due to the first property) whose x - and z -marginals are $(Q_n)_X$ and $(Q_n)_Z$ respectively (due to the second property) and is absolutely continuous with respect to Q_n^* (due to the third property) hence is in \mathcal{Q}_n and is at distance ϵ from Q_n^* (due to the fourth property).

Pick any

$$\gamma < \min \left\{ \frac{2}{5} \min_{(x, z) \in \text{supp}(Q^*)} Q^*(x, z), \frac{\epsilon}{2|\mathcal{X}||\mathcal{Z}|} \right\}. \quad (181)$$

Then, $\exists n_0(\gamma)$ such that for $\forall n > n_0, |Q_n^* - Q^*| \leq \gamma/2$ and $|Q_n - Q| \leq \gamma/2$. Therefore, in particular,

$$|(Q_n^*)_X - Q_X^*| = |(Q_n^*)_X - Q_X| \leq \gamma/2 \quad (182)$$

and

$$|(Q_n)_X - Q_X| \leq \gamma/2 \quad (183)$$

which, together with the triangle inequality imply,

$$|(Q_n^*)_X - (Q_n)_X| \leq \gamma. \quad (184)$$

Similarly,

$$|(Q_n^*)_Z - (Q_n)_Z| \leq \gamma. \quad (185)$$

Let G be the “connectivity graph of the joint distribution Q_n^* , namely the bipartite graph $G = (\mathcal{X}, \mathcal{Z}, \mathcal{E})$ where there is an edge between x and z , $(x, z) \in \mathcal{E}$, iff $Q_n^*(x, z) > 0$. Suppose G is connected (we discuss what happens if this is not the case later). Then, it certainly has a spanning tree. Let $T = (\mathcal{X}, \mathcal{Z}, \mathcal{E}')$, $\mathcal{E}' \subseteq \mathcal{E}$ be one such tree, and pick any vertex $v \in \mathcal{X} \cup \mathcal{Z}$ as the root. Suppose the tree has height H . Let $\mathcal{V} = \mathcal{X} \cup \mathcal{Z}$ be the set of all nodes of G and \mathcal{V}_h denote the set of vertices at height h in the tree. For every node $v \in \mathcal{V}_h$,

let $p(v) \in \mathcal{V}_{h-1}$ be the parent of v and $\mathcal{K}(v) = \{u \in \mathcal{V}_{h+1} : (v, u) \in \mathcal{E}'\}$ be the children of v (with $\mathcal{K}(v) = \emptyset$ for the leaves). Consider the following algorithm to associate a value δ_e to each edge of the tree:

- 1: **for** $h = H$ **to** 1 **do**
- 2: **for** $v \in \mathcal{V}_h$ **do**
- 3: $\delta_e \leftarrow \delta(v) - \sum_{u \in \mathcal{K}(v)} \delta(v, u)$
- 4: **end for**
- 5: **end for**

where in line 3 we have used the generic notation

$$\delta(v) = \begin{cases} \delta_X(x), & \text{if } v \in \mathcal{X}, \\ \delta_Z(z), & \text{if } v \in \mathcal{Z}. \end{cases} \quad (186)$$

Finally, set

$$\delta(x, z) = \begin{cases} \delta_e & \text{if } (x, z) \in \mathcal{E}' \\ 0 & \text{otherwise.} \end{cases} \quad (187)$$

$\delta : \mathcal{X} \times \mathcal{Z} \rightarrow \mathbb{R}$, as obtained above, satisfies all the desired four properties:

- 1) is trivial: if (x, z) is not on the tree $n\delta(x, z) = 0$, otherwise $\delta(x, z) = \delta_e$, $e = (x, z)$ and δ_e is the sum of multiples of $\frac{1}{n}$ thus is itself a multiple of $\frac{1}{n}$.
- 2) holds by construction except for the root. Without loss of generality suppose the root is a vertex $x_0 \in \mathcal{X}$. Then,

$$\sum_{x, z} \delta(x, z) = \sum_z \delta_Z(z) = 0. \quad (188)$$

(since δ_Z is the difference of two distributions). Therefore,

$$0 = \sum_z \delta(x_0, z) + \sum_{x \neq x_0} \sum_z \delta(x, z) \quad (189)$$

$$= \sum_z \delta(x_0, z) + \sum_{x \neq x_0} \delta_X(x) \quad (190)$$

which implies

$$\sum_z \delta(x_0, z) = - \sum_{x \neq x_0} \delta_X(x) = \delta_X(x_0) \quad (191)$$

again since δ_X is the difference of two distributions.

Moreover by induction on T , we can prove that for every edge $e \in \mathcal{E}'$,

$$\delta_e \leq \sum_{v \in T_e} |\delta(v)|, \quad (192)$$

where T_e is the sub-tree rooted at the highest vertex of e . By extending the sum in (192) to the entire tree and noting that $\sum_x |\delta_X(x)| + \sum_z |\delta_Z(z)| = |(Q_n^*)_X - (Q_n)_X| + |(Q_n^*)_Z - (Q_n)_Z| \leq 2\gamma$, we get the following weaker bound: $\forall (x, z) \in \mathcal{X} \times \mathcal{Z}$,

$$|\delta(x, z)| \leq 2\gamma, \quad (193)$$

which implies the last two properties:

- 3) follows since $\delta(x, z) = 0$ if $Q_n^*(x, z) = 0$ (as $(x, z) \notin \mathcal{E} \supset \mathcal{E}'$) and

$$Q_n^*(x, z) + \delta(x, z) \geq Q_n^*(x, z) - 2\gamma \quad (194)$$

$$\geq Q^*(x, z) - \frac{5}{2}\gamma \geq 0 \quad (195)$$

because of (181).

4) follows since

$$|\delta| \leq 2|\mathcal{X}||\mathcal{Z}|\gamma \leq \epsilon \quad (196)$$

(again because of (181)).

Disconnected G: Suppose for some n , G is not connected and is rather union of two connected components (the proof can be generalized to any finite number of components easily). This means that we can partition \mathcal{X} and \mathcal{Z} into two subsets as $\mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2$, $\mathcal{X}_1 \cap \mathcal{X}_2 = \emptyset$ and $\mathcal{Z} = \mathcal{Z}_1 \cup \mathcal{Z}_2$, $\mathcal{Z}_1 \cap \mathcal{Z}_2 = \emptyset$ where $\mathcal{E} = \text{supp}(Q_n^*) \subseteq (\mathcal{X}_1 \times \mathcal{Z}_1) \cup (\mathcal{X}_2 \times \mathcal{Z}_2)$.

This, together with the choice of γ in (181) implies $\text{supp}(Q_n^*) \subseteq (\mathcal{X}_1 \times \mathcal{Z}_1) \cup (\mathcal{X}_2 \times \mathcal{Z}_2)$ and hence, $\forall n$, $\text{supp}(Q_n^*) \subseteq (\mathcal{X}_1 \times \mathcal{Z}_1) \cup (\mathcal{X}_2 \times \mathcal{Z}_2)$.

For $\forall n \in \mathbb{N}$, let

$$\lambda_n \triangleq \sum_{(x,z) \in \mathcal{X}_1 \times \mathcal{Z}_1} Q_n^*(x,z) = 1 - \sum_{(x,z) \in \mathcal{X}_2 \times \mathcal{Z}_2} Q_n^*(x,z). \quad (197)$$

Note that $n\lambda_n$ is an integer and by assumption $\lim_{n \rightarrow \infty} \lambda_n = Q_X^*(\mathcal{X}_1) = Q_X(\mathcal{X}_1) > 0$ (if this is not the case we should have started with a smaller \mathcal{X}) thus $\lim_{n \rightarrow \infty} n\lambda_n = \infty$. Similarly, we conclude that $n(1 - \lambda_n)$ is an integer-valued sequence that goes to infinity as n grows.

Let

$$Q_n^{*'}(x,z) \triangleq \frac{Q_n^*(x,z)}{\lambda_n} \mathbb{1}\{(x,z) \in \mathcal{X}_1 \times \mathcal{Z}_1\} \quad \text{and} \quad (198)$$

$$Q_n^{*''}(x,z) \triangleq \frac{Q_n^*(x,z)}{\overline{\lambda_n}} \mathbb{1}\{(x,z) \in \mathcal{X}_2 \times \mathcal{Z}_2\}, \quad (199)$$

(where we have used the shorthand notation $\overline{\lambda_n} = 1 - \lambda_n$) and observe that

$$\begin{aligned} D(Q_n^* \parallel (Q_n^*)_X \times W) \\ = \lambda_n D(Q_n^{*'} \parallel (Q_n^{*'})_X \times W) + \overline{\lambda_n} D(Q_n^{*''} \parallel (Q_n^{*''})_X \times W). \end{aligned} \quad (200)$$

Note that $Q_n^{*'}$ (resp. $Q_n^{*''}$) is an $n\lambda_n$ -type (resp. $n\overline{\lambda_n}$ -type). Define also

$$Q'_n(x,z) \triangleq \frac{Q_n(x,z)}{\lambda_n} \mathbb{1}\{(x,z) \in \mathcal{X}_1 \times \mathcal{Z}_1\} \quad \text{and} \quad (201)$$

$$Q''_n(x,z) \triangleq \frac{Q_n(x,z)}{\overline{\lambda_n}} \mathbb{1}\{(x,z) \in \mathcal{X}_2 \times \mathcal{Z}_2\}, \quad (202)$$

and note that Q'_n (resp. Q''_n) is also an $n\lambda_n$ -type (resp. an $n\overline{\lambda_n}$ -type).

Our argument for connected G shows that there exists a sequence of $n\lambda_n$ -types $\{Q_n^{*'} \in \mathcal{Q}_{n\lambda_n}\}_{n \in \mathbb{N}}$ such that $\forall n$, $(Q_n^{*'})_X = (Q'_n)_X$, $(Q_n^{*'})_Z = (Q'_n)_Z$ and $\lim_{n \rightarrow \infty} |Q_n^{*'} - Q'_n| = 0$. Similarly, there exists a sequence of $n\overline{\lambda_n}$ -types $\{Q_n^{*''} \in \mathcal{Q}_{n\overline{\lambda_n}}\}_{n \in \mathbb{N}}$ such that $\forall n$, $(Q_n^{*''})_X =$

$(Q''_n)_X$, $(Q_n^{*''})_Z = (Q''_n)_Z$ and $\lim_{n \rightarrow \infty} |Q_n^{*''} - Q''_n| = 0$. Therefore,

$$D(Q^* \parallel Q_X^* \times W) = \lim_{n \rightarrow \infty} D(Q_n^* \parallel (Q_n^*)_X \times W) \quad (203)$$

$$= \lim_{n \rightarrow \infty} \left\{ \lambda_n D(Q_n^{*'} \parallel (Q_n^{*'})_X \times W) + \overline{\lambda_n} D(Q_n^{*''} \parallel (Q_n^{*''})_X \times W) \right\} \quad (204)$$

$$= \lim_{n \rightarrow \infty} \left\{ \lambda_n D(Q_n^{*'} \parallel (Q_n^{*'})_X \times W) + \overline{\lambda_n} D(Q_n^{*''} \parallel (Q_n^{*''})_X \times W) \right\} \quad (205)$$

$$\geq \lim_{n \rightarrow \infty} \left\{ \lambda_n \phi_{n\lambda_n}(Q'_n) + \overline{\lambda_n} \phi_{n\overline{\lambda_n}}(Q''_n) \right\}. \quad (206)$$

Moreover, using the same reasoning as we had to prove convexity of ϕ (see (167)) it follows that

$$\lambda_n \phi_{n\lambda_n}(Q'_n) + \overline{\lambda_n} \phi_{n\overline{\lambda_n}}(Q''_n) \geq \phi_n(\lambda_n Q'_n + \overline{\lambda_n} Q''_n) = \phi(Q_n). \quad (207)$$

Therefore, continuing (206), we will again have

$$\phi(Q) = D(Q^* \parallel Q_X^* \times W) \geq \lim_{n \rightarrow \infty} \phi_n(Q_n) \quad (208)$$

which concludes the proof. \blacksquare

2) *Proof of (30):* Now we are ready to prove (30). We need to show that

$$\lim_{n \rightarrow \infty} E_{s,n}^{c.c.}(P_n, W, R) = E_s^{c.c.}(P_X, W, R) \quad (209)$$

for any sequence of n -types, $P_n \in \mathcal{P}_n(\mathcal{X})$ that converge to P_X . Let

$$\tilde{V}_n \triangleq \arg \min_{\substack{V: \mathcal{X} \rightarrow \mathcal{Z}; \\ P_X \times V \in \mathcal{P}_n(\mathcal{X} \times \mathcal{Z})}} \{D(V \parallel W | P_n) + [R - g_n(V \parallel W | P_n)]^+\} \quad (210)$$

and (by passing to a subsequence if necessary) $\tilde{V} \triangleq \lim_{n \rightarrow \infty} \tilde{V}_n$. We know that $P_n \times V_n \ll P_n \times W$, thus, by the continuity of divergence and (171),

$$\begin{aligned} \lim_{n \rightarrow \infty} E_{s,n}^{c.c.}(P_n, W, R) \\ = D(\tilde{V} \parallel W | P_X) + [R - g(\tilde{V} \parallel W | P_X)]^+ \end{aligned} \quad (211)$$

$$\geq \min_{V: \mathcal{X} \rightarrow \mathcal{Z}} \{D(V \parallel W | P_X) + [R - g(V \parallel W | P_X)]^+\} \quad (212)$$

$$= E_s^{c.c.}(P_X, W, R). \quad (213)$$

On the other side, let

$$V^* = \arg \min_{V: \mathcal{X} \rightarrow \mathcal{Z}} \{D(V \parallel W | P_X) + [R - g(V \parallel W | P_X)]^+\}. \quad (214)$$

There exists a sequence of stochastic matrices $V_n^* : \mathcal{X} \rightarrow \mathcal{Z}$ such that, (a) $P_n \times V_n^* \in \mathcal{P}_n(\mathcal{X} \times \mathcal{Z})$, (b) $\lim_{n \rightarrow \infty} |P_n \times V_n^* - P_X \times V^*| = 0$, and (c) $\forall n$, $P_n \times V_n^* \ll P_n \times W$. Accepting this momentarily, by continuity of $D(V \parallel W | P)$ and (171), we have

$$\begin{aligned} E_s^{c.c.}(P_X, W, R) \\ = \lim_{n \rightarrow \infty} \{D(V_n^* \parallel W | P_n) + [R - g_n(V_n^* \parallel W | P_n)]^+\} \end{aligned} \quad (215)$$

$$\geq \lim_{n \rightarrow \infty} E_{n,s}^{c.c.}(P_n, W, R) \quad (216)$$

which, together with (213) yields (209).

Existence of such V_n^* s already follows from the algorithm we presented in the proof of Lemma 9 or more simply from the following argument: We assumed (without essential loss of generality) that $\text{supp}(P_X) = \mathcal{X}$. Therefore, the assumption $\lim_{n \rightarrow \infty} |P_n - P_X| = 0$, implies $\forall x \in \mathcal{X}$, $\lim_{n \rightarrow \infty} P_n(x) = P_X(x) > 0$, thus $\lim_{n \rightarrow \infty} nP_n(x) = +\infty$. Pick $\epsilon > 0$. Therefore $\exists n_0(\epsilon)$ such that $\forall n > n_0$, $|P_X - P_n| \leq \epsilon/2$. Moreover, for each x , $V^*(\cdot|x)$ is the limit point of a sequence of n -types on $\text{supp}(V^*(\cdot|x))$. Therefore, for every $x \in \mathcal{X}$, $\exists n_x(\epsilon)$ such that for $\forall n > n_x$, there exists an $nP_n(x)$ -type $V_n^*(\cdot|x)$ such that $|V^*(\cdot|x) - V_n^*(\cdot|x)| \leq \epsilon/2$ and $V_n^*(\cdot|x) \ll V^*(\cdot|x)$. Finally, we observe that $P_n \times V_n^*$ is a n -type and for $n > \max\{n_0, \max_{x \in \mathcal{X}} n_x\}$, $|P_n \times V_n^* - P_X \times V^*| \leq \epsilon$.

C. Strict Monotonicity of $E_s^{\text{i.i.d.}}$ and $E_s^{\text{c.c.}}$ in R

That $E_s^{\text{i.i.d.}}$ is strictly increasing in R for $R > I(P_X, W)$ can be easily seen through the form of (32): $E_s^{\text{i.i.d.}}$ is the supremum of affine functions of R thus is convex in R . On the other side, since $F_0(P_X, W, \lambda)$ is a convex function of λ passing through the origin with slope $I(P_X, W)$, $E_s^{\text{i.i.d.}}(P_X, W, R)$ starts to increase above 0 once R exceeds $I(P_X, W)$ which means it will be strictly increasing for $R > I(P_X, W)$.

We only need to prove the claim for $E_s^{\text{c.c.}}$. (This proof may also be used to show $E_s^{\text{i.i.d.}}$ is strictly increasing in R , replacing g with f .) Note that

$$E_s^{\text{c.c.}}(P_X, W, R) = \min \left\{ \min_{V: g(V\|W|P_X) \geq R} D(V\|W|P_X), \min_{V: g(V\|W|P_X) \leq R} \{D(V\|W|P_X) + R - g(V\|W|P_X)\} \right\}. \quad (217)$$

We first show that for $R > I(P_X, W)$,

$$\begin{aligned} E_s^{\text{c.c.}}(P_X, W, R) &= \min_{V: g(V\|W|P_X) \leq R} \{D(V\|W|P_X) + R - g(V\|W|P_X)\} \\ &= R + \min_{V: g(V\|W|P_X) \leq R} \{D(V\|W|P_X) - g(V\|W|P_X)\} \end{aligned} \quad (218)$$

$$= R + \min_{V: g(V\|W|P_X) \leq R} \{D(V\|W|P_X) - g(V\|W|P_X)\} \quad (219)$$

This follows since for $R > I(P_X, W)$,

$$\begin{aligned} &\min_{V: g(V\|W|P_X) \geq R} D(V\|W|P_X) \\ &= \min_{V: g(V\|W|P_X) = R} D(V\|W|P_X) \end{aligned} \quad (220)$$

Let us first prove (220): Suppose this is not the case, i.e., there exists V^* with $g(V^*\|W|P_X) > R$ such that $D(V^*\|W|P_X) \leq D(V\|W|P_X)$ for every V with $g(V\|W|P_X) \geq R$. We can safely assume that $P_X \times V^* \ll P_X \times W$ (otherwise $D(V\|W|P_X) = +\infty$ for all V such that $g(V\|W|P_X) \geq R$ and (219) automatically follows). Let $V_\lambda \triangleq \lambda V^* + (1 - \lambda)W$, for $\lambda \in [0, 1]$. It is easy to check that $\forall \lambda \in [0, 1]$: $P_X \times V_\lambda \ll P_X \times W$, thus the mapping $\lambda \mapsto g(V_\lambda\|W|P_X)$ is continuous by the continuity of g (see Lemma 8) on the interval $[0, 1]$. We know that $g(V_1\|W|P_X) = g(V^*\|W|P_X) > R$ and $g(V_0\|W|P_X) = g(W\|W|P_X) = I(P_X, W) < R$. Therefore,

there exists $\beta \in (0, 1)$ for which $g(V_\beta\|W|P_X) = R$. On the other side, the convexity of divergence implies

$$D(V_\beta\|W|P_X) \leq \beta D(V^*\|W|P_X) + (1 - \beta) D(W\|W|P_X) \quad (221)$$

$$< D(V^*\|W|P_X) \quad (222)$$

since $\beta < 1$. This contradicts the optimality of V^* .

Now, we show that $E_s^{\text{c.c.}}(P_X, W, R') > E_s^{\text{c.c.}}(P_X, W, R)$ for $R' > R > I(P_X, W)$. Let

$$V^* = \arg \min_{V: g(V\|W|P_X) \leq R'} \{D(V\|W|P_X) - g(V\|W|P_X)\}. \quad (223)$$

If $g(V^*\|W|P_X) \leq R$, then

$$E_s^{\text{c.c.}}(P_X, W, R') = R' + D(V^*\|W|P_X) - g(V^*\|W|P_X) \quad (224)$$

$$= R' + \min_{V: g(V\|W|P_X) \leq R} \{D(V\|W|P_X) - g(V\|W|P_X)\} \quad (225)$$

$$> R + \min_{V: g(V\|W|P_X) \leq R} \{D(V\|W|P_X) - g(V\|W|P_X)\} \quad (226)$$

$$= E_s^{\text{c.c.}}(P_X, W, R) \quad (227)$$

which proves the claim.

Otherwise, we have $R < g(V^*\|W|P_X) \leq R'$. Consider once again the family of stochastic matrices defined as $V_\lambda \triangleq \lambda V^* + (1 - \lambda)W$. We know $P_X \times V^* \ll P_X \times W$ (for if it is not, $D(V^*\|W|P_X) = +\infty$ and $g(V^*\|W|P_X) = -\infty$ which means the exponent is infinity which is contradiction since $E_s^{\text{c.c.}}(P_X, W, R') \leq R' - I(P_X, W)$ by taking $V = W$ in (219)). Using the same reasoning as above, since $g(V_1\|W|P_X) > R$ and $g(V_0\|W|P_X) = I(P_X, W) < R$ one can find $\beta \in (0, 1)$ such that $g(V_\beta\|W|P_X) = R$ and

$$D(V_\beta\|W|P_X) \leq \beta D(V^*\|W|P_X). \quad (228)$$

Moreover, we know that

$$D(V_\beta\|W|P_X) = R + [D(V_\beta\|W|P_X) - g(V_\beta\|W|P_X)] \quad (229)$$

$$\geq R + \min_{V: g(V\|W|P_X) \leq R} \{D(V\|W|P_X) - g(V\|W|P_X)\} \quad (230)$$

$$= E_s^{\text{c.c.}}(P_X, W, R). \quad (231)$$

One the other side,

$$E_s^{\text{c.c.}}(P_X, W, R') = R' + D(V^*\|W|P_X) - g(V^*\|W|P_X) \quad (232)$$

$$\stackrel{(a)}{\geq} D(V^*\|W|P_X) \quad (233)$$

$$\stackrel{(b)}{\geq} \frac{1}{\beta} D(V_\beta\|W|P_X) \quad (234)$$

$$\stackrel{(c)}{\geq} \frac{1}{\beta} E_s^{\text{c.c.}}(P_X, W, R) \quad (235)$$

$$\stackrel{(d)}{>} E_s^{\text{c.c.}}(P_X, W, R), \quad (236)$$

where (a) follows since $g(V^* \| W | P_X) \leq R'$, (b) follows from (228) and (c) from (231) and finally (d) holds since $\beta < 1$ and $E_s^{c.c.}(P_X, W, R) > 0$.

D. Alternative form of $E_s^{i.i.d.}$

Let $P_{XZ} = P_X \times W$ again. Using the fact that $\max\{a, 0\} = \max_{0 \leq \lambda \leq 1} \lambda a$,

$$\begin{aligned} & \min_Q \{D(Q \| P_{XZ}) + [R - f(Q \| P_{XZ})]^+\} \\ &= \min_Q \left\{ D(Q \| P_{XZ}) + \max_{0 \leq \lambda \leq 1} \lambda [R - f(Q \| P_{XZ})] \right\} \end{aligned} \quad (237)$$

$$= \min_Q \max_{0 \leq \lambda \leq 1} \{ \lambda R + D(Q \| P_{XZ}) - \lambda f(Q \| P_{XZ}) \} \quad (238)$$

$$\stackrel{(a)}{=} \max_{0 \leq \lambda \leq 1} \min_Q \{ \lambda R + D(Q \| P_{XZ}) - \lambda f(Q \| P_{XZ}) \} \quad (239)$$

$$= \max_{0 \leq \lambda \leq 1} \left\{ \lambda R + \min_Q \{ D(Q \| P_{XZ}) - \lambda f(Q \| P_{XZ}) \} \right\} \quad (240)$$

$$\stackrel{(b)}{=} \max_{0 \leq \lambda \leq 1} \{ \lambda R - F_0(P_X, W, \lambda) \} \quad (241)$$

where (a) follows since $D(Q \| P_{XZ}) - \lambda f(Q \| P_{XZ})$ is convex in Q (recall that f is linear in Q) and (b) since

$$\begin{aligned} & D(Q \| P_{XZ}) - \lambda f(Q \| P_{XZ}) \\ &= \sum_{x,z} Q(x, z) \log \frac{Q(x, z)}{P_{XZ}(x, z)^{1+\lambda} P_X(x)^{-\lambda} P_Z(z)^{-\lambda}} \end{aligned} \quad (242)$$

$$\stackrel{(*)}{\geq} -\log \sum_{x,z} P_{XZ}(x, z)^{1+\lambda} P_X(x)^{-\lambda} P_Z(z)^{-\lambda} \quad (243)$$

$$= F_0(P_X, W, \lambda), \quad (244)$$

with equality in $(*)$ iff $Q(x, z) \propto P_{XZ}(x, z)^{1+\lambda} P_X(x)^{-\lambda} P_Z(z)^{-\lambda}$. ■

APPENDIX C PROOF OF (34)

Taking $V' = V$ in (31b), we have $g(V \| W | P) \leq I(P, V)$, thus,

$$R - g(V \| W | P_X) \geq R - I(P_X, V). \quad (245)$$

Therefore,

$$\begin{aligned} & E_s^{c.c.}(P_X, W, R) \\ &= \min_V \{ D(V \| W | P_X) + [R - g(V \| W | P_X)]^+ \} \end{aligned} \quad (246)$$

$$\geq \min_V \{ D(V \| W | P_X) + [R - I(P_X, V)]^+ \} \quad (247)$$

$$\stackrel{(a)}{=} \min_V \{ D(V \| W | P_X) + \max_{0 \leq \lambda \leq 1} \{ \lambda R - \lambda I(P_X, V) \} \} \quad (248)$$

$$\stackrel{(b)}{=} \max_{0 \leq \lambda \leq 1} \{ \lambda R + \min_V \{ D(V \| W | P_X) - \lambda I(P_X, V) \} \} \quad (249)$$

where (a) follows since $[a]^+ = \max_{0 \leq \lambda \leq 1} \lambda a$ and (b) by observing that $D(V \| W | P_X) - \lambda I(P_X, V)$ is convex in V for

$\lambda \leq 1$ (and linear in λ). The latter holds since $I(P_X, V) = \min_{Q_Z \in \mathcal{P}(\mathcal{Z})} D(V \| Q_Z | P_X)$, therefore,

$$\begin{aligned} & D(V \| W | P_X) - \lambda I(P_X, V) \\ &= \max_{Q_Z \in \mathcal{P}(\mathcal{Z})} \{ D(V \| W | P_X) - \lambda D(V \| Q_Z | P_X) \} \end{aligned} \quad (250)$$

$$= \max_{Q_Z} \sum_{x,z} P_X(x) V(z|x) \log \frac{V(z|x)^{1-\lambda}}{W(z|x) Q_Z(z)^{-\lambda}} \quad (251)$$

$$= \frac{1}{t} \max_{Q_Z} \sum_{x,z} P_X(x) V(z|x) \log \frac{V(z|x)}{W(z|x)^t Q_Z(z)^{1-t}}. \quad (252)$$

where we have defined $t \triangleq \frac{1}{1-\lambda}$ in the last step. The objective function inside the max in (252) is convex in V and since the supremum of convex functions is still convex, the convexity of $D(V \| W | P_X) - \lambda I(P_X, V)$ in V follows. It can also be seen that the objective function is concave in Q_Z for $\lambda > 0$ (i.e. $t > 1$). Using this observation we have

$$\begin{aligned} & \min_V \{ D(V \| W | P_X) - \lambda I(P_X, V) \} \\ &= \frac{1}{t} \min_V \max_{Q_Z} \sum_{x,z} P_X(x) V(z|x) \log \frac{V(z|x)}{W(z|x)^t Q_Z(z)^{1-t}} \end{aligned} \quad (253)$$

$$= \frac{1}{t} \max_{Q_Z} \min_V \sum_{x,z} P_X(x) V(z|x) \log \frac{V(z|x)}{W(z|x)^t Q_Z(z)^{1-t}} \quad (254)$$

$$\stackrel{(a)}{=} \max_{Q_Z} \left\{ -\frac{1}{t} \sum_x P_X(x) \log \sum_z W(z|x)^t Q_Z(z)^{1-t} \right\} \quad (255)$$

$$\stackrel{(b)}{\geq} \max_{Q_Z} \left\{ -\frac{1}{t} \log \sum_x P_X(x) \sum_z W(z|x)^t Q_Z(z)^{1-t} \right\} \quad (256)$$

$$= -\min_{Q_Z} \left\{ \frac{1}{t} \log \sum_z Q_Z(z)^{1-t} \sum_x P_X(x) W(z|x)^t \right\} \quad (257)$$

where (a) and (b) follow by the concavity of logarithm. KKT conditions imply the solution to the minimization of (257) is

$$Q_Z(z) = c \left(\sum_x P_X(x) W(z|x)^t \right)^{1/t} \quad (258)$$

with $c^{-1} = \sum_z (\sum_x P_X(x) W(z|x)^t)^{1/t}$. Plugging this into the objective function of (257) and replacing $t = \frac{1}{1-\lambda}$, we have

$$\begin{aligned} & \min_V \{ D(V \| W | P_X) - \lambda I(P_X, V) \} \\ &= -\log \sum_z \left(\sum_x P_X(x) W(z|x)^{\frac{1}{1-\lambda}} \right)^{1-\lambda} \end{aligned} \quad (259)$$

$$= -E_0(P_X, W, \lambda). \quad (260)$$

Plugging (260) into (249) proves the claim. ■

APPENDIX D

NUMERICAL EVALUATION OF THE SECRECY EXPONENTS

A. Computing $E_s^{\text{i.i.d.}}$ and $E_s^{\text{c.c.}}$

Both $E_s^{\text{i.i.d.}}$ and $E_s^{\text{c.c.}}$ can be easily evaluated via the expressions (32) and (33) using the fact that both F_0 and E_0 (defined in (32b) and (33b) respectively) are convex in λ , and pass through the origin with slope $I(P_X, W)$.

For instance to evaluate $E_s^{\text{i.i.d.}}$ we know that

- 1) for $R \leq I(P_X, W) = \frac{\partial}{\partial \lambda} F_0(P_X, W, \lambda)|_{\lambda=0}$, $E_s(P_X, W, R) = 0$;
- 2) for $I(P_X, W) < R < \frac{\partial}{\partial \lambda} F_0(P_X, W, \lambda)|_{\lambda=1}$, the pairs $R, E_s^{\text{i.i.d.}}$ are related parametrically as

$$R(\lambda) = \frac{\partial}{\partial \lambda} F_0(P_X, W, \lambda) \quad (261a)$$

$$E_s(\lambda) = \lambda R(\lambda) - F_0(P_X, W, \lambda) \quad (261b)$$

for the range of $\lambda \in [0, 1]$;

- 3) finally, if $R \geq F'_0(1)$,

$$E_s(P_X, W, R) = R - F_0(P_X, W, 1). \quad (262)$$

It is clear that to evaluate $E_s^{\text{c.c.}}$, one has to follow precisely the same steps replacing F_0 with E_0 .

B. Computing $E_s^{\text{c.c.}}$

To compute $E_s^{\text{c.c.}}$ (defined in (31)), one has to solve two minimizations. Namely, that of (31a) and that of (31b). The latter turns out to be efficiently solvable using standard convex optimization tools.

Fix $Q_Z \in \mathcal{P}(\mathcal{Z})$ (to be set to $P_X \circ V$ to compute $g(V\|W|P_X)$). We have:

$$\min_{V': P_X \circ V' = Q_Z} D(V'\|W|P_X) = \min_{V'} \left\{ D(V'\|W|P_X) + \max_{\rho \in \mathbb{R}^{|\mathcal{Z}|}} \sum_z \rho_z [Q_Z(z) - (P_X \circ V')(z)] \right\} \quad (263)$$

$$= \max_{\rho \in \mathbb{R}^{|\mathcal{Z}|}} \left\{ \min_{V'} \left\{ D(V'\|W|P_X) - \sum_{x,z} P_X(x) V'(z|x) \rho_z \right\} + \sum_z \rho_z Q_Z(z) \right\}, \quad (264)$$

where $\rho \triangleq (\rho_1, \dots, \rho_{|\mathcal{Z}|})$ and the last equality follows since $D(V\|W|P_X)$ is convex in V and the second term is linear in V . Moreover, the inner unconstrained minimization has the value

$$\min_{V'} \left\{ D(V'\|W|P_X) - \sum_{x,z} P_X(x) V'(z|x) \rho_z \right\} = \min_{V'} \sum_{x,z} P_X(x) V'(z|x) \log \frac{V'(z|x)}{W(z|x) \exp(\rho_z)} \quad (265)$$

$$= - \sum_x P_X(x) \log \sum_z W(z|x) \exp(\rho_z), \quad (266)$$

by choosing $V'(z|x) \propto W(z|x) \exp(\rho_z)$. Plugging this into (264), we get

$$\min_{V': P_X \circ V' = Q} D(V'\|W|P_X) = \max_{\rho \in \mathbb{R}^{|\mathcal{Z}|}} \left\{ \sum_z \rho_z Q_Z(z) - \sum_x P_X(x) \log \sum_z W(z|x) \exp(\rho_z) \right\}. \quad (267)$$

Remark. Using Hölder's inequality, it can be checked that the objective function of (267) is concave in ρ , thus can be efficiently maximized using standard numerical methods.

Proof: Since the first sum in the objective function of (267) is linear in ρ it is sufficient to prove that the function

$$\rho \mapsto \sum_x P_X(x) \log (W(z|x) \exp(\rho_z)) \quad (268)$$

is convex in ρ . Fix $t \in [0, 1]$ and $\rho, \rho' \in \mathbb{R}^{|\mathcal{Z}|}$. For every $x \in \mathcal{X}$, Hölder's inequality implies

$$\begin{aligned} \sum_z W(z|x) \exp(t\rho_z + (1-t)\rho'_z) &= \sum_z W(z|x)^t \exp(t\rho_z) \cdot W(z|x)^{1-t} \exp((1-t)\rho'_z) \\ &\leq \left(\sum_z W(z|x) \exp(\rho_z) \right)^t \cdot \left(\sum_z W(z|x) \exp(\rho'_z) \right)^{1-t} \end{aligned} \quad (269)$$

$$\leq \left(\sum_z W(z|x) \exp(\rho_z) \right)^t \cdot \left(\sum_x W(z|x) \exp(\rho'_z) \right)^{1-t} \quad (270)$$

Taking the logarithm of both sides, multiplying by $P_X(x)$, and finally summing over x proves the claim. ■

Finally, for small alphabet sizes that we have considered in Section IV-B, we can solve the minimization of (31a) via exhaustive search.

APPENDIX E

PROOF OF LEMMA 6

- (i) The linearity of expectation shows that \bar{P}_{Z^n} as defined in (12) is the expectation of the non-negative random variable $P_{C_n}(z^n)$ (defined in (8)). Therefore, $\bar{P}_{Z^n}(z^n) = 0$ implies $P_{C_n}(z^n) = 0$ almost surely.
- (ii) Pick z^n and \tilde{z}^n that have the same type. Therefore, there exists a permutation, call it $\pi: \mathcal{Z}^n \rightarrow \mathcal{Z}^n$, such that $\tilde{z}^n = \pi(z^n)$ and $z^n = \pi^{-1}(\tilde{z}^n)$. Then,

$$\bar{P}_{Z^n}(\tilde{z}^n) = \sum_{x^n} P_{X^n}(x^n) W^n(\tilde{z}^n|x^n) \quad (271)$$

$$\stackrel{(a)}{=} \sum_{\tilde{x}^n} P_{X^n}(\pi(\tilde{x}^n)) W^n(\pi(z^n)|\pi(\tilde{x}^n)) \quad (272)$$

$$\stackrel{(b)}{=} \sum_{\tilde{x}^n} P_{X^n}(\tilde{x}^n) W^n(z^n|\tilde{x}^n) = \bar{P}_{Z^n}(z^n). \quad (273)$$

where in (a) we have taken $x^n = \pi(\tilde{x}^n)$ and (b) follows since $P_{X^n}(x^n)$ only depends on the type of x^n (and by construction \tilde{x}^n and $\pi(\tilde{x}^n)$ have the same type) and similarly $W^n(\pi(z^n)|\pi(\tilde{x}^n)) = W^n(z^n|\tilde{x}^n)$.

- (iii) We have

$$\bar{P}_{Z^n}(z^n) = \sum_{x^n \in \mathcal{X}^n} P_{X^n}(x^n) W^n(z^n|x^n) \quad (274)$$

$\bar{P}_{Z^n}(z^n) > 0$ implies there exists at least one sequence $x_0^n \in \text{supp}(P_{X^n})$ for which $W^n(z^n|x_0^n) > 0$. Therefore, $W^n(z^n|x_0^n) > W_{\min}^n$. Thus (274) yields

$$\bar{P}_{Z^n}(z^n) \geq P_{X^n}(x_0^n) W_{\min}^n. \quad (275)$$

For i.i.d. random coding ensemble, $P_{X^n}(x^n) = P_X^n(x^n) \geq P_{\min}^n$ and for the constant-composition random coding ensemble, $P_{X^n}(x^n) = 1/|\mathcal{T}_{P_X}^n| \geq (1/|\mathcal{X}|)^n$ (since $\mathcal{T}_{P_X}^n \subseteq \mathcal{X}^n$). ■

APPENDIX F

PROOF OF LEMMA 7

Take $U \triangleq \frac{A}{\mathbb{E}[A]}$ so that $\mathbb{E}[U] = 1$. We shall prove that

$$c(\theta) (\text{var}(U) - \tau_\theta(U)) \leq \mathbb{E}[U \ln(U)] \leq \text{var}(U). \quad (276)$$

The claim then follows by noting that $\mathbb{E}[A \ln(A/\mathbb{E}[A])] = \mathbb{E}[A] \mathbb{E}[U \ln(U)]$ and $\text{var}(A) = \text{var}(U)/(\mathbb{E}[A])^2$.

We first have

$$\mathbb{E}[U \ln(U)] = \mathbb{E}[U \ln(U) - (U - 1)] \quad (277)$$

$$\leq \mathbb{E}[(U - 1)^2] = \text{var}(U), \quad (278)$$

since $u \ln(u) - (u - 1) \leq (u - 1)^2$. On the other hand,

$$u \ln(u) - (u - 1) \geq c(\theta)(u - 1)^2 \mathbb{1}\{u \leq \theta + 1\}. \quad (279)$$

This follows by observing that $\frac{u \ln(u) - (u - 1)}{(u - 1)^2}$ is a decreasing function of u (see Lemma 10 below). Thus,

$$\mathbb{E}[U \ln(U)] \geq c(\theta) \int_0^{\theta+1} (u - 1)^2 dF_U(u). \quad (280)$$

where $F_U(u)$ is the cumulative distribution function of u .

Furthermore,

$$\int_0^{\theta+1} (u - 1)^2 dF_U(u) = \text{var}(U) - \int_{\theta+1}^{+\infty} (u - 1)^2 dF_U(u) \quad (281)$$

Let $v \triangleq u - 1$ for the sake of brevity and denote by $\bar{F}_V(v) \triangleq \Pr\{V > v\} = \Pr\{U > v + 1\}$ the complementary distribution function of V . Then,

$$\int_{\theta+1}^{+\infty} (u - 1)^2 dF_U(u) = \int_{\theta}^{+\infty} v^2 dF_V(v) \quad (282)$$

$$= [-v^2 \bar{F}_V(v)]_{\theta}^{+\infty} + 2 \int_{\theta}^{+\infty} v \bar{F}_V(v) dv \quad (283)$$

$$\stackrel{(*)}{=} \theta^2 \bar{F}_V(\theta) + 2 \int_{\theta}^{+\infty} v \bar{F}_V(v) dv. \quad (284)$$

The equality in (*) follows since we assumed the variance of U exists. This proves (276). ■

Lemma 10. For $t \geq 0$,

- (i) the mapping $t \mapsto \frac{t \ln(t) - (t - 1)}{t - 1}$ is increasing in t ;
- (ii) the mapping $t \mapsto \frac{t \ln(t) - (t - 1)}{(t - 1)^2}$ is decreasing in t .

Proof:

(i)

$$\frac{\partial}{\partial t} \left\{ \frac{t \ln(t) - (t - 1)}{t - 1} \right\} = \frac{(t - 1) - \ln(t)}{(t - 1)^2} \geq 0 \quad (285)$$

since $\ln(t) \leq t - 1$.

(ii)

$$\frac{\partial}{\partial t} \left\{ \frac{t \ln(t) - (t - 1)}{(t - 1)^2} \right\} = \frac{2(t - 1) - (t + 1) \ln(t)}{(t - 1)^3} \leq 0, \quad (286)$$

since for $t \geq 1$, $\ln(t) \geq 2\frac{t-1}{t+1}$ while for $t \leq 1$, $\ln(t) \leq 2\frac{t-1}{t+1}$. The latter follows since $\ln(t) - 2\frac{t-1}{t+1}$ equals 0 at $t = 1$ and has derivative

$$\frac{(t - 1)^2}{t(t + 1)^2} \geq 0. \quad \blacksquare$$

APPENDIX G

PROOF OF (48)

We have

$$p_Q(z^n) = \sum_{x^n \in \mathcal{X}^n} \mathbb{1}\{(x^n, z^n) \in \mathcal{T}_Q^n\} P_{X^n}(x^n) \quad (287)$$

$$= \frac{P_{X^n}(\mathcal{T}_{Q_X}^n)}{|\mathcal{T}_{Q_X}^n|} \sum_{x^n \in \mathcal{X}^n} \mathbb{1}\{(x^n, z^n) \in \mathcal{T}_Q^n\} \quad (288)$$

since $P_{X^n}(x^n)$ only depends on the type of x^n . On the other side, we have

$$|\mathcal{T}_Q^n| = \sum_{z^n \in \mathcal{Z}^n} \sum_{x^n \in \mathcal{X}^n} \mathbb{1}\{(x^n, z^n) \in \mathcal{T}_Q^n\} \quad (289)$$

The value of the inner sum in (289) only depends on the type of z^n (this can be easily checked using the same type of argument as we had in Appendix E part (ii)) and, clearly, is zero if $Q_Z \neq \hat{Q}_{z^n}$. Thus

$$|\mathcal{T}_Q^n| = |\mathcal{T}_{Q_Z}^n| \mathbb{1}\{Q_Z = \hat{Q}_{z^n}\} \sum_{x^n \in \mathcal{X}^n} \mathbb{1}\{(x^n, z^n) \in \mathcal{T}_Q^n\}. \quad (290)$$

Plugging (290) into (288) yields (48). ■

APPENDIX H

PROOF OF (55)

We only prove (55a) (as (55b) is trivial). (We omit the dependence on z^n throughout the proof for notational brevity.)

$$\begin{aligned} \text{var}(L_1) &= \sum_{Q \in \mathcal{Q}'_n} \frac{1}{M^2} \ell(Q)^2 \text{var}(N_Q) \\ &+ \sum_{\substack{(Q_1, Q_2) \in \mathcal{Q}'_n{}^2 \\ Q_1 \neq Q_2}} \frac{1}{M^2} \ell(Q_1) \ell(Q_2) \text{cov}(N_{Q_1}, N_{Q_2}) \end{aligned} \quad (291)$$

$$\begin{aligned} &\stackrel{(*)}{=} \frac{1}{M} \sum_{Q \in \mathcal{Q}'_n} \ell(Q)^2 p_Q (1 - p_Q) \\ &- \frac{1}{M} \sum_{\substack{(Q_1, Q_2) \in \mathcal{Q}'_n{}^2 \\ Q_1 \neq Q_2}} \ell(Q_1) \ell(Q_2) p_{Q_1} p_{Q_2}, \end{aligned} \quad (292)$$

where (*) follows since $\text{var}(N_Q) = M p_Q (1 - p_Q)$ and $\text{cov}(N_{Q_1}, N_{Q_2}) = -M p_{Q_1} p_{Q_2}$. Moreover,

$$\begin{aligned} &\sum_{\substack{(Q_1, Q_2) \in \mathcal{Q}'_n{}^2 \\ Q_1 \neq Q_2}} \ell(Q_1) \ell(Q_2) p_{Q_1} p_{Q_2} \\ &= \sum_{Q_1 \in \mathcal{Q}'_n} \ell(Q_1) p_{Q_1} \sum_{Q_2 \in \mathcal{Q}'_n \setminus \{Q_1\}} \ell(Q_2) p_{Q_2} \end{aligned} \quad (293)$$

$$= \sum_{Q_1 \in \mathcal{Q}'_n} \ell(Q_1) p_{Q_1} \left(\mathbb{E}[L_1] - p_{Q_1} \ell(Q_1) \right). \quad (294)$$

Using the above in (292) we get,

$$\begin{aligned}
& \text{var}(L_1) \\
&= \frac{1}{M} \sum_{Q \in \mathcal{Q}'_n} \ell(Q) p_Q \left[(1 - p_Q) \ell(Q) - (\mathbb{E}[L_1] - p_Q \ell(Q)) \right] \\
&= \frac{1}{M} \sum_{Q \in \mathcal{Q}'_n} \ell(Q) p_Q [\ell(Q) - \mathbb{E}[L_1]] \\
&= \frac{1}{M} \sum_{Q \in \mathcal{Q}'_n} \ell(Q)^2 p_Q - \frac{1}{M} \mathbb{E}[L_1]^2. \quad \blacksquare
\end{aligned} \tag{295}$$

APPENDIX I PROOF OF (121)

Equation (119) immediately implies

$$\begin{aligned}
\mathbb{E}[D(P_{C_n} \| \bar{P}_{Z^n})] &\leq \sum_{Q \in \mathcal{P}_n(\mathcal{X} \times \mathcal{Z})} \exp\{-nD(Q \| Q_X \times W)\} \\
&\quad \times P_{X^n}(\mathcal{T}_{Q_X}^n) \min\left\{1, \frac{\ell(Q)}{M}\right\}. \tag{297}
\end{aligned}$$

It remains to show

$$\begin{aligned}
\mathbb{E}[D(P_{C_n} \| \bar{P}_{Z^n})] &\geq \sum_{Q \in \mathcal{P}_n(\mathcal{X} \times \mathcal{Z})} \exp\{-nD(Q \| Q_X \times W)\} \\
&\quad \times P_{X^n}(\mathcal{T}_{Q_X}^n) \min\left\{1, \frac{\ell(Q)}{M}\right\}, \tag{298}
\end{aligned}$$

to establish (121).

Equation (119) means there exists a sub-exponentially increasing sequence $\beta(n)$ (which depends only on $|\mathcal{X}|$ and $|\mathcal{Z}|$) such that

$$\begin{aligned}
& \beta(n) \left[\mathbb{E}[D(P_{C_n} \| \bar{P}_{Z^n})] + \frac{\log(e)}{M} \right] \\
&\geq \sum_{Q \in \mathcal{P}_n(\mathcal{X} \times \mathcal{Z})} \exp\{-nD(Q \| Q_X \times W)\} \\
&\quad \times P_{X^n}(\mathcal{T}_{Q_X}^n) \min\left\{1, \frac{\ell(Q)}{M}\right\}. \tag{299}
\end{aligned}$$

Since the union of n -types is dense in $\mathcal{P}(\mathcal{X} \times \mathcal{Z})$, for large enough n , there exists an n -type that is as close as desired to the joint distribution $P_X \times W$. More precisely, for every $\epsilon > 0$, there exists $n_0(\epsilon)$ such that $\forall n > n_0(\epsilon)$, there exists $Q_n \in \mathcal{P}_n(\mathcal{X} \times \mathcal{Z})$ for which $I(Q_n) \geq I(P_X, W) - \epsilon$, $D(Q_n \| (Q_n)_X \times W) \leq \epsilon/2$ and $P_{X^n}(\mathcal{T}_{(Q_n)_X}^n) > \exp(-n\epsilon/2)$. Indeed, taking $Q_n = P_n \times W_n$, where P_n is an n -type quantization of P_X for the i.i.d. random coding ensemble and W_n is the quantization of W such that $W_n(\cdot|x)$ is a $nP_n(x)$ -type yields all desired properties.

Note also that

$$\ell(Q) \geq \exp(n\omega(Q)) |\mathcal{T}_{Q_Z}^n| \tag{300}$$

$$\stackrel{(*)}{\geq} (n+1)^{-|\mathcal{Z}|} \exp(n[\omega(Q) + H(Q_Z)]) \tag{301}$$

$$= (n+1)^{-|\mathcal{Z}|} \exp(n[I(Q) - D(Q \| Q_X \times W)]), \tag{302}$$

where $(*)$ follows from [22, Lemma 2.3]. Let

$$\epsilon \triangleq \min\{R/2, I(P_X, W)/4\} > 0 \tag{303}$$

and observe that for all $n \geq n_0(\epsilon)$ with Q_n as described above

$$\ell(Q_n) \geq (n+1)^{-|\mathcal{Z}|} \exp\{n(I(P_X, W) - 2\epsilon)\}. \tag{304}$$

Consequently, the term corresponding to $Q = Q_n$ in the summation of (299) is lower-bounded as

$$\begin{aligned}
& \exp(-nD(W_n \| W | P_n)) P_{X^n}(\mathcal{T}_{P_n}^n) \min\left\{1, \frac{\ell(Q_n)}{M}\right\} \\
&\geq (n+1)^{-|\mathcal{Z}|} \exp\{-n(\epsilon + [R - I(P_X, W) + 2\epsilon]^+)\} \\
&\geq (n+1)^{-|\mathcal{Z}|} \exp\{-n(R - \epsilon)\}. \tag{305}
\end{aligned}$$

$$\geq (n+1)^{-|\mathcal{Z}|} \exp\{-n(R - \epsilon)\}. \tag{306}$$

The last inequality follows because of the choice of ϵ in (303). Obviously, $\exists n_1(\epsilon, |\mathcal{X}|, |\mathcal{Z}|)$ such that $\forall n \geq n_1$,

$$\begin{aligned}
\beta(n) \frac{\log(e)}{M} &= \beta(n) \log(e) \exp(-nR) \\
&\leq \frac{1}{2} (n+1)^{-|\mathcal{Z}|} \exp(-n(R - \epsilon)). \tag{307}
\end{aligned}$$

This, together with (306) implies for $n \geq n_2 \triangleq \max\{n_0, n_1\}$,

$$\begin{aligned}
\beta(n) \frac{\log(e)}{M} &\leq \frac{1}{2} \exp(-nD(W_n \| W | P_n)) P_{X^n}(\mathcal{T}_{P_n}^n) \\
&\quad \times \min\left\{1, \frac{\ell(Q_n)}{M}\right\}. \tag{308}
\end{aligned}$$

Using (308) in (298) (and multiplying the summands corresponding to $Q \neq Q_n$ by $\frac{1}{2}$) we conclude that for $n \geq n_2$,

$$\begin{aligned}
& \beta(n) \mathbb{E}[D(P_{C_n} \| \bar{P}_{Z^n})] \\
&\geq \frac{1}{2} \sum_{Q \in \mathcal{P}_n(\mathcal{X} \times \mathcal{Z})} \exp\{-nD(Q_{Z|X} \| W | Q_X)\} \\
&\quad \times P_{X^n}(\mathcal{T}_{Q_X}^n) \min\left\{1, \frac{\ell(Q)}{M}\right\}. \tag{309}
\end{aligned}$$

Take

$$\beta'(n) \triangleq \begin{cases} +\infty & \text{if } n < n_2 \\ 2\beta(n) & \text{otherwise.} \end{cases} \tag{310}$$

Therefore, $\forall n$,

$$\begin{aligned}
& \beta'(n) \mathbb{E}[D(P_{C_n} \| \bar{P}_{Z^n})] \\
&\geq \sum_{Q \in \mathcal{P}_n(\mathcal{X} \times \mathcal{Z})} \exp\{-nD(Q_{Z|X} \| W | Q_X)\} \\
&\quad \times P_{X^n}(\mathcal{T}_{Q_X}^n) \min\left\{1, \frac{\ell(Q)}{M}\right\}. \tag{311}
\end{aligned}$$

We finally have

$$\limsup_{n \rightarrow \infty} \frac{1}{n} \log \beta'(n) = \limsup_{n \rightarrow \infty} \frac{1}{n} \log \beta(n) = 0 \tag{312}$$

by assumption and that β' only depends on $|\mathcal{X}|$, $|\mathcal{Z}|$, R , P_X , and W (because n_2 only depends on these parameters). Therefore, (311) establishes (298) and concludes the proof. \blacksquare

REFERENCES

- [1] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.
- [3] J. L. Massey, "A simplified treatment of wyner's wire-tap channel," in *Proceedings of Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, Oct. 1983, pp. 268–276.
- [4] M. R. Bloch and J. N. Laneman, "Strong secrecy from channel resolvability," *IEEE Transactions on Information Theory*, vol. 59, no. 12, pp. 8077–8098, Dec. 2013.
- [5] I. Csiszár, "Almost independence and secrecy capacity," *Problems of Information Transmission*, vol. 32, no. 1, pp. 40–47, 1996.
- [6] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Advances in Cryptology — EURO-CRYPT 2000*, ser. Lecture Notes in Computer Science, B. Preneel, Ed., vol. 1807. Springer-Verlag, May 2000, pp. 351–368.
- [7] M. Hayashi, "General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channel," *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1562–1575, Apr. 2006.
- [8] —, "Exponential decreasing rate of leaked information in universal random privacy amplification," *IEEE Transactions on Information Theory*, vol. 57, no. 6, pp. 3989–4001, Jun. 2011.
- [9] M. Hayashi and R. Matsumoto, "Secure multiplex coding with dependent and non-uniform multiple messages," in *Proceedings of Annual Allerton Conference on Communication, Control, and Computing*, Oct. 2012, pp. 954–959.
- [10] T. S. Han, H. Endo, and M. Sasaki, "Reliability and secrecy functions of the wiretap channel under cost constraint," *IEEE Transactions on Information Theory*, vol. 60, no. 11, pp. 6819–6843, Nov. 2014.
- [11] M. Bastani Parizi and E. Telatar, "On the secrecy exponent of the wire-tap channel," in *Proceedings of IEEE Information Theory Workshop (ITW)*, Oct. 2015, pp. 287–291.
- [12] J. Körner and A. Sgarro, "Universally attainable error exponents for broadcast channels with degraded message sets," *IEEE Transactions on Information Theory*, vol. 26, no. 6, pp. 670–679, Nov. 1980.
- [13] M. Hayashi and R. Matsumoto, "Universally attainable error and information exponents, and equivocation rate for the broadcast channels with confidential messages," in *Proceedings of Annual Allerton Conference on Communication, Control, and Computing*, Sep. 2011, pp. 439–444.
- [14] J. Hou and G. Kramer, "Informational divergence approximations to product distributions," in *Proceedings of Canadian Workshop on Information Theory (CWIT)*, Jun. 2013, pp. 76–81.
- [15] —, "Effective secrecy: Reliability, confusion and stealth," in *Proceedings of IEEE International Symposium on Information Theory (ISIT)*, Jun. 2014, pp. 601–605.
- [16] T.-H. Chou, V. Y. F. Tan, and S. C. Draper, "The sender-excited secret key agreement model: Capacity, reliability, and secrecy exponents," *IEEE Transactions on Information Theory*, vol. 61, no. 1, pp. 609–627, Jan. 2015.
- [17] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.
- [18] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography—part I: Secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.
- [19] M. Hayashi, "Tight exponential analysis of universally composable privacy amplification and its applications," *IEEE Transactions on Information Theory*, vol. 59, no. 11, pp. 7728–7746, Nov. 2013.
- [20] M. Hayashi and V. Y. F. Tan, "Equivocations and exponents under various rényi information measures," in *Proceedings of IEEE International Symposium on Information Theory (ISIT)*, Jun. 2015, pp. 281–285.
- [21] I. Csiszár, "The method of types," *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2505–2523, Oct. 1998.
- [22] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 2nd ed. Cambridge University Press, 2011.
- [23] A. D. Wyner, "The common information of two dependent random variables," *IEEE Transactions on Information Theory*, vol. 21, no. 2, pp. 163–179, Mar. 1975.
- [24] T. S. Han and S. Verdú, "Approximation theory of output statistics," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 752–772, May 1993.
- [25] P. Cuff, "Distributed channel synthesis," vol. 59, no. 11, pp. 7071–7096, Nov. 2013.
- [26] R. G. Gallager, *Information Theory and Reliable Communication*. New York, NY, USA: John Wiley & Sons, Inc., 1968.
- [27] —, "The random coding bound is tight for the average code," *IEEE Transactions on Information Theory*, vol. 19, no. 2, pp. 244–246, Mar. 1973.
- [28] N. Shulman, "Communication over an unknown channel via common broadcasting," Ph.D. dissertation, Department of Electrical Engineering Systems, Tel Aviv University, 2003.
- [29] N. Merhav, "Exact random coding error exponents of optimal bin index decoding," *IEEE Transactions on Information Theory*, vol. 60, no. 10, pp. 6024–6031, Oct. 2014.
- [30] —, "Statistical physics and information theory," *Foundations and Trends in Communications and Information Theory*, vol. 6, no. 1–2, pp. 1–212, 2009. [Online]. Available: <http://dx.doi.org/10.1561/01000000052>
- [31] P. Cuff, "Soft covering with high probability," in *Proceedings of IEEE International Symposium on Information Theory (ISIT)*, Jul. 2016, pp. 2963–2967.